BAB II

TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Keamanan Aplikasi Web

Keamanan aplikasi *web* merupakan serangkaian tindakan yang diambil untuk melindungi situs *web* dari berbagai ancaman dikenal sebagai keamanan *web.* (Khatib Sulaiman & Pakuan, U., 2024) Salah satu komponen terpenting dari pengembangan perangkat lunak kontemporer adalah keamanan aplikasi *web.* Risiko serangan siber meningkat seiring dengan adopsi layanan berbasis *web*. Serangan aplikasi *web* dapat mengakibatkan kerugian *moneter,* pencuria informasi pribadi.

Keamanan aplikasi *web* dapat dipahami melalui tiga aspek utama, yaitu *confidentialty, integrity,* dan *availability*. *Confidentiality* berkaitan dengan perlindungan data agar tidak diakses pihak yang tidak berwenang. *Integrity* berkaitan dengan jaminan bahwa data tidak dimodifikasi secara tidak sah. *Availability* berkaitan dengan ketersediaan layanan agar dapat digunakan oleh pengguna yang berhak. Ketiga aspek tersebut menjadi dasar dalam menilai dampak dari setiap temuan keamanan

2.1.2 Web Application Penetration Testing

Web Application Penetration Testing (WAPT) adalah metode yang mensimulasikan serangan dari sudut pandang pihak ketiga yang tidak berwenang untuk menemukan dan menilai kerentanan dalam aplikasi *web.* Untuk

mengidentifikasi kelemahan dari keamanan yang dapat dimanfaatkan oleh penyerang, pendekatan ini menggunakan berbagai metode dan sumber daya. Menemukan kelemahan sebelum orang yang tidak bertanggung jawab dapat memanfaatkannya. (Widianto et al., 2025)

2.1.3 OWASP Top 10

Meningkatkan keamanan perangkat lunak adalah tujuan dari *Open Web Application Security Project* (OWASP) OWASP top 10 mencantumkan sepuluh ancaman keamanan aplikasi *web* terpenting, (Setiawan et al., n.d.-a) Daftar ini yang membantu pengembang dan pakar keamanan menemukan dan memperbaiki kerentanan, sering diperbarui berdasarkan data dan tren serangan tertentu. Berikut daftar 10 ancaman OWASP top 10 :

a. *Broken access Control*

Broken access control adalah ancaman keamanan aplikasi *web* yang paling umum dan berbahaya. Kerentanan ini terjadi ketika aplikasi tidak menerapkan pembatasan akses yang tepat, sehingga pengguna dapat mengakses data atau fitur yang seharusnya tidak mereka miliki.

b. Cryptographic Failures

Cryptographic failures adalah salah satu ancaman serius yang bisa menyebabkan pencurian data sensitif. Untuk mencegahnya, gunakan standar enkripsi yang kuat, kelola kunci dengan baik, dan pastikan semua data dalam transit serta penyimpanan yang aman.

c. Injection

Injeksi merupakan cara untuk memasukan data ke dalam aplikasi yang kemudian diinterpretasikan atau dieksekusi oleh aplikasi. Tahap ini memastikan penyerang tidak dapat mengirim data yang tidak sah kedalam aplikasi. Contoh dari kasus injeksi yaitu penyerang memodifikasi nilai parameter ‘id’ pada *browser* untuk mengirim ‘or’1’=’1.

d. Insecure Design

Insecure design adalah masalah arsitektur yang tidak bisa diperbaiki hanya dengan *patching code.* Untuk menghindarinya, keamanan harus menjadi bagian integral dalam perancangan aplikasi sejak awal.

e. Security Misconfiguration

Security misconfiguration adalah kesalahan umum yang sering terjadi karena kelalaian dalam konfigurasi keamanan. Untuk mencegahnya, selalu ubah pengaturan default, nonaktifkan fitur yang tidak diperlukan, perbarui sistem secara berkala, dan lakukan audit keamanan secara rutin.

f. Vulnerable and Outdated Components

Vulnerable and outdated components bisa menjadi celah yang berbahaya bagi *hacker* jika tidak di lakukan pembaruan dengan benar. Untuk menghindarinya, pastikan sistem selalu menggunakan versi terbaru, hapus komponen yang tidak diperlukan, dan gunakan alat pemantauan keamanan.

g. Identification and Authentication Failures

Identification and authentication failures adalah kelemahan dalam sistem identifikasi dan otentikasi yang dapat dieksploitasi oleh penyerang untuk mendapatkan akses ilegal ke akun atau data sensitif.

h. Software and Data Integrity Failures

Software and data integrity failures terjadi ketika aplikasi atau data tidak memiliki keamanan yang baik untuk mencegah modifikasi yang tidak sah. Serangan seperti *supply chain attack, dependency confusion,* dan CI/CD *pipeline hijacking* bisa menyebabkan dampak yang luas.

i. Security Logging Monitoring Failures

Security logging monitoring failures terjadi ketika sistem gagal mencatat dan mendeteksi aktivitas mencurigakan, sehingga serangan dapat berlangsung tanpa terdeteksi. Serangan seperti *brute force, malware,* dan pencurian data bisa memiliki dampak yang leih besar jika tidak ada mekanisma *logging and monitoring.* .

j. Server-Side Request Forgery (SSRF)

Server-side request forgery adalah kelemahan keamanan di mana seorang penyerang dapat mengeskploitasi aplikasi untuk mengirimkan permintaan HTTP yang tidak sah dari server ke sumber lain, termasuk sumber internal yang tidak dapat diakses langsung oleh penyerang. SSRF sering terjadi jika aplikasi menerima input dari pengguna untuk membuat permintaan ke sumber eksternal tanpa validasi yang memadai.

2.1.4 *Security Misconfiguration*

Security Misconfiguration adalah kondisi ketika aplikasi, server, *framework*, *database,* atau komponen pendukung tidak dikonfigurasi secara aman. Sebagai contoh tidak diterapkannya *security headers,* munculnya informasi server melalui *header respons,* konfigurasi *cookie* yang tidak aman, direktori yang dapat diakses publik, atau penggunaan konfigurasi *default*. Pada aplikasi *web* moderen, *securitty misconfiguration* sering menjadi celah awal yang dapat memperbesar dampak serangan lain.

2.1.5 *Session Management* dan *Atribut Cookie*

Session managament adalah mekanisme yang digunakan aplikasi untuk mempertahankan status autentikasi dan identitas pengguna selama berinteraksi dengan sistem. *Cookie* sesi yang tidak dikonfigurasi secara aman dapat meningkatkan risiko pencurian atau penyalahgunaan sesi. Atribut *HTTPOnly* digunakan untuk mencegah akses *cookie* oleh skrip sisi klien, *Secure* digunakan agar *cookie* hanya dikirim melalui koneksi HTTPS, sedangkan *SameSite* digunakan untuk membatasi pengiriman *cookie* dalam konteks lintas situs.

2.1.6 *Clickjacking* dan *Security Headers*

Clickjacking adalah serangan yang memanfaatkan pemuatan halaman target di dalam *frame* atau *iframe* milik pihak lain sehingga pengguna dapat diarahkan untuk melakukan klik pada elemen yang tidak disadari. Risiko ini dapat dikurangi dengan menerapkan *X-Frame-Option* atau *Content-Security-Policy* melalui direktif *frame ancestors.* Oleh karena itu, keberadaan atau ketiadaan *header* tersebut menjadi indikator penting dalam pengujian keamanan antarmuka aplikasi *web.*

2.1.7 Validasi *True Positive* dan *Negative*

Hasil pemindaian otomatis tidak selalu menunjukan kerentanan yang benar-benar dapat dieksploitasi. Oleh karena itu, validasi manual diperlukan untuk menentukan apakah suatu *alert* merupakan *true positive, false positive,* atau hanya *informational finding. True positive* berarti temuan berhasil dibuktikan melalui pengujian terkendali. *False positive* berarti *alert* muncul tetapi tidak terbukti sebagai celah. *Negative finding* berarti skenario pengujian tidak menemukan kelemahan pada aspek yang diuji.

2.1.8 Analisis Dampak CIA

Analisis dampak CIA digunakan untuk melihat pengaruh setiap temuan terhadap kerahasiaan, integritas, dan ketersediaan sistem. Temuan seperti *cookie* yang dapat diakses terhadap identitas sesi. Temuan *Clickjacking* berkaitan dengan *integrity* dan *confidentiality* karena dapat memanipulasi interaksi pengguna dan membuka peluang penyalahgunaan tindakan pada aplikasi

2.2 Penelitian Terkait

2.2.1 State of The Art

Berikut ini beberapa penelitian terdahulu yang dilakukan dalam metode *Web Application Penetration testing* berdasarkan OWASP Top 10, berikut penelitian terkait disajikan pada Tabel

Tabel 2.1 Penelitian Terkait *(State of the art)*

No.	Nama, Tahun Peneliti	Judul	Metode/Solusi	Hasil Penelitian
1	(Fernanda Tinambunan, Achmad Junaidi, Agung Mustika Rizki 2024)	Pengujian Sistem Informasi Akademik Universitas X Melalui Pendekatan *Penetration Testing* Berdasarkan OWASP Top 10	Metode OWASP & *Penetration Testing*	-Hasil *Scanning* menggunakan OWAS ZAP menemukan 23 celah keamanan pada sistem informasi akademik universitas X, dengan 20 celah masuk dalam kategori OWASP Top 10. -Dari 23 celah keamanan, terdapat 5 celah berisiko tinggi, 4 celah berisiko sedang, 9 celah berisiko rendah, dan 5 celah informasi. -Pengujian eksploitasi dilakukan pada celah keamanan dengan risiko tinggi dan sedang, seperti *Cross site scripting, SQL Injection, Path Traversal, Content Security Policy, Clickjaking,* dan *Vulnerable Javascript Library.*
2	(Ichsan Octama Riandhanu 2022)	Analisis Metode *Open Web Application Security Project* (OWASP) Menggunakan *Penetration Testing* pada keamanan *website* absensi	Metode *Penetration Testing* dan OWASP Top 10	- Hasil pemindaian dengan netsparker menemukan 20 kerentanan yang masuk dalam kategori OWASP Top 10, dengan rincian 1 kerentanan kritis, 3 kerentanan tinggi, 4 kerentanan sedang, dan 7 kerentanan rendah.

				- Kerentanan yang ditemukan antara lain *Sensitive Data Exposure, Security Misconfiguration,* dan *Using Components with Known Vulnerabilities* - Kesimpulan bahwa analisis keamanan menggunakan metode OWASP terbukti efektif dalam mengidentifikasi dan mengevaluasi kerentanan keamanan pada *website* absensi perusahaan X
3	(Dimas Febriyan Priambodo, Asep Dadan Firmansyah, Muhammad Hasbi 2023)	*Penetration Testing Web* XYZ Berdasarkan OWASP *Risk Rating*	Metode *Penetration Testing* dengan pendekatan OWASP top 10	-Hasil pemindaian kerentanan menggunakan OWAS ZAP dan vega menemukan 9 jenis kerentanan dengan rincian 2 kerentanan *high,* 1 kerentanan *medium,* dan 6 kerentanan *low.* - Setelah dilakukan validasi, terdapat 2 kerentanan *true positive,* yaitu *Vulnerable JS Library* dan *Cookie Without Same Site Attribute.* -Kesimpulan bahwa penerapan OWASP Top 10 dan OWASP *Risk Rating Methodology* terbukti efektif dalam mengidentifikasi dan mengevaluasi kerentanan keamanan pada *website* "XYZ".
4	(Ade Putra Armadhani, Dicky Nofriansyah Khairi Ibnutama 2022)	Analisis Keamanan Untuk Mengetahuai *Vulnerability* Pada DVWA *Lab Testing* Menggunakan *Penetration Testing Standart* OWASP	Penelitian data *Collecting, Penetration Testing,* OWASP	- Pada uji kerentanan c*ommand execution,* ditemukan celah dimana pengguna dapat menjalankan perintah linux pada *server*. Solusi yang diberikan adalah membatasi perintah yang dapat dieksekusi - Pada uji kerentanan *SQL Injection,* ditemukan celah dimana pengguna dapat menyisipkan *query SQL* yang valid untuk membaca informasi *database.*Solusi yang diberikan adalah menggunakan fungsi *mysql_real_escape_string()* dan *stripslashes()* untuk memfilter input.

				-Dapat disimpulkan bahwa metode OWASP dapat diterapkan dengan baik untuk mengidentifikasi dan menyelesaikan masalah keamanan pada aplikasi *web* DVWA *Lab Testing*
5	(Ela Nurelasari, Difa Gumilang Al Farabi 2024)	Analisis Keamanan Sistem *Website* Menggunakan Metode *Oen Web Application Security Project* (OWASP) Pada SIMANTEP.ID	Analisis data OWASP, dan *Tools* OWASZap	-Hasil pemindaian menggunakan OWASZap menemukan 10 tanda bahaya (*alert)* pada *website* Simantep.id, dengan rincian 3 kerentanan level *medium* 3 kerentanan level *low,* dan 4 kerentanan kerentanan level *informational*. -Kerentanan yang di temukan berdasarkan kategori OWASP Top 10 adalah : *Broken Access Control (level medium), Insecure Design (level low), Security Misconfiguration (level low), Software and Data Integrity Failures (level low)* -Kesimpulan bahwa metode OWASP Top 10 masih relevan untuk menguji keamanan *website* dan prinsip keamanan CIA (*Confidentiality, Integrity, Availability*) telah diterapkan pada *website* Simantep.id
6	(Yudiana, Anggi Elanda, Robby Lintang Buana 2021)	Analisis kualitas keamanan sistem informasi *e-office* berbasis *website* pada STIMIK rosma dengan menggunakan OWASP Top 10	OWASP Top 10, OWASPZAP dan *Acunetix Web Vulnerability Scanner*	Menggunakan *Acunetix,* ditemukan 3 kerentanan dengan tingkat kerentanan sedang, rendah, dan informatif. Menggunakan OWASPZAP, ditemukan 13 kerentanan termasuk yang masuk kategori OWASP Top 10. Perlu perbaikan lebih lanjut terhadap sistem informasi *e-office* oleh pengembang untuk meningkatkan kualitas keamanan.
7	(Maulana Pandudinata,	Analisis kerentanan *website* SMA Negeri 2 Amlapura menggunakan metode OWASP	OWASP, OWASPZAP	Ditemukan 2 faktor untuk memperkirakan *Likehood* dan *Impcat.* Dari masing-masing faktor terdapat 3 tingkat risiko yaitu tinggi, sedang, dan rendah. Hasil

	Farid Ridho 2024)	(*open web application security project)*		penilaian risiko dapat membantu mengambil tindakan untuk mencegah dan mengatasi risiko pada sistem.
8	(Zidan Faizi, Purwantoro, Azhari Ali Ridha 2023)	Analisis Keamanan Aplikasi Berbasis *Web* di Lingkungan BPS RI. Studi Kasus : Aplikasi *Web* Jafung BPS	Penelitian Kualitatif, PTES, OWASP *Risk Rating Methodology*	-Hasil pengujian penetrasi menemukan 37 kerentanan pada aplikasi *web* jafung BPS, dengan rincian 7 kerentenan *level informational*, 14 kerentanan *level low,* dan 16 kerentanan *level informational.* -Dari 37 kerentanan tersebut, 13 risiko ekpolitasi berhasil dilakukan, yang terdiri dari 3 skenario XSS, 1 skenario *clickjacking,* 3 skenario IDOR, 4 skenario *sensitive data exposure,* dan 2 skenario tambahan (CSRF dan *file upload vulnerability)*. -Hasil penilain risiko kerentanan menunjukan aplikasi *web* jafung BPS memiliki nilai *likelihood factors* 5,21 dan nilai *impact factors* 3,06 sehingga masuk dalam kategori risiko kerentanan *medium*.
9	(Hermawan Setiawan Lytio Enggar Erlangga, Syubbanul Siddiq, Yusuf Atha Gunawan 2023)	Analisis Kerawanan Pada Aplikasi *Website* Menggunakan Standar OWASP Top 10 Untuk penilaian *Risk Rating*	OWASP *Risk Rating Methodology*	-Dari hasil S*canning Vulnerability* terakhir, ditemukan 13 kerentanan pada aplikasi *website* SMAN “ABC” dengan kategori tinggi hingga rendah. -Berdasarkan penilaian kerentanan yang terdeteksi, diperoleh skala 5,72 untuk kemungkinan kerentanan dapat di eksploitasi oleh penyerang (*likelihood)* dan skala 3,315 untuk dampak terhadap proses bisnis (*impact)*. -Dapat disimpulkan bahwa aplikasi *website* SMAN “ABC” meiliki risiko keamanan yang tergolong medium, sehingga perlu dilakukan perbaikan dan peningkatan keamanan.

10	(Ahmad Alfian Chandra, Ahmad Turmudi Zy, Agung Nugroho 2024)	Penerapan Teknik *Penetration Testing* terhadap *Cross-Site Scripting* (XSS) dalam pengembangan *website*	OWASZAP untuk mendeteksi kerentanan XSS	Ditemukannya kerentanan XSS pada parameter "*name"* dan *"comment" website* target. Penggunaan htmlsspecialchars() efektif mencegah eksekusi kode berbahaya dan meningkatkan keamanan *website. Penetration Testing* terbukti efektif untuk mendeteksi kerentanan keamanan pada *website.*
11	(Urshila Ravindran, Raghu Vamsi Potukuchi 2022)	*A Review on Web Application Vulnerability Assessment and Penetreation Testing*	*Literature Review*	Evaluasi berbagai metode pengujian keamanan aplikasi web.
12	(Janstipen Roy Mansen Sagala, Yusnia Budiarti, Rosi Kusuma Serli 2024)	Analisis Keamanan Aplikasi *Website* Kecamatan Cibodas Tanggerang Dengan Metode *Open Web Application Security Project*	*Penetration Testing*	Identifikasi kerentanan keamanan dalam *website* pemerintah
13	(Bad'ul Hilmi Arromdoni, Mandahadi Kusuma, Bambang Sugiantoro 2024)	*Web Application Vulnerability Analysis Using the* OWASP *Method (Case Study:* OJS CSFD UIN Sunan Kalijaga Yogyakarta)	Analisis Keamanan *Web*	Mengidentifikasi dan mengurangi kerentanan keamanan dalam system OJS
14	(Chinekezi Chinyere Echefunna,	*Evaluation of Information Security in Web Application Through Penetration Testing*	OWASP *Risk Assessment*	Evaluasi keamanan aplikasi *web* berdasarkan metodologi risiko OWASP

	Jude Osamor, Celestine Iwendi 2024	*Techniques Using* OWASP *Risk Methodology*		
15	(Aida Fitriya Sebrina, Achmad Junaidi, Andreas Nugroho Sihananto 2024)	*Testing* Posketanmu *Website with Google Penetration Testing and* OWASP Top 10	*Google Penetarion Testing*	Menggunakan *Google Dork* dan OWASP untuk mengidentifikasi kerentanan keamanan
16	(M. Sakthivel, S. Sivanantham, N. Bharathiraja 2024)	*Ensuring Web Application Security: An* OWASP *Driven Development Methodology*	OWASP Top 10 *Framework*	Penerapan metodologi pengembangan berbasis keamanan OWASP
17	(Yoel Armando, Rosalina Rosalina 2023)	*Penetration Testing* Tanggerang *City Web Application With Implementing* OWASP Top 10 *Web Security Risk Framework*	*Penetration Testing*	Identifikasi dan mitigasi risiko keamanan berbasis OWASP Top 10
18	(Mistry Mahima Ankit 2024)	*Unveling the Underbelly of Web Application Vulnerabilities: A critical Exploration*	Analisis Keamanan Web	Mengidentifikasi kelemahan utama dalam keamanan aplikasi *web*
19	(Yuvraj Singh 2024)	*WebSec: Exploring and Modulating Vulnerabilities*	Eksplorasi Kerentanan	Evaluasi teknik mitigasi ancaman siber dalam aplikasi *web*

20	(Madhuri N. Gedam, Bandu B. Meshram 2023)	*Web Application Top* 10 OWASP *Attacks and Defence Mechanism*	Studi Keamanan *Web*	Identifikasi dan mitigasi serangan siber berdasarkan OWASP Top 10
21	(Malak Saleh Aljabri, Maryam AlDossary, Noor Al-Homeed 2022)	*Testing and Exploiting Tools to Improve* OWASP *Top Ten Security Vulnerabilities Detection*	Eksploitasi & Deteksi	Pengembangan alat untuk meningkatkan deteksi ancaman OWASP Top 10
22	(Sonali Patil, Mandaar Rao, Lavitra Misal 2023)	*A Review of the* OWASP Top 10 *Web Application Security Risks and Best Practices for Mitigating These Risks*	*Literature Review*	Tinjauan metode terbaik untuk mengatasi risiko keamanan OWASP Top 10
23	(Muhamad Agreinda Helmiawan, Esa Firmansyah, Irfan Fadil 2020)	*Analysis of Web Security Using Open Web Application Security Project* 10	OWASP *Security Audit*	Analisis keamanan *web* berdasarkan OWASP Top 10
24	(E. Altulaihan, Abrar Alismail, Mounir Frikha 2023)	*A Survey on Web Application Penetration Testing*	*Literature Review*	Studi komprehensif tentang teknik dan pendekatan *pentesting web*

25	(Petar T. Lachkov, Lo'ai Tawalbeh, Smriti Bhatt 2022)	*Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing*	Simulasi & Pengujian Keamanan	Identifikasi dan mitigasi kerentanan aplikasi melalui simulasi serangan.
26	(Ravinder Singh, Manan Gupta, Dipak Raghunath Patil 2024)	*Analysis of Web Application Vulnerabilities using Dynamic Application Security Testing*	*Dynamic Application Security Testing (*DAST)	Evaluasi efektivitas DAST dalam mendeteksi kerentanan OWASP Top 10
27	(Jyoti Rawat, Indrajeet Kumar, Mohd Halim, Mohd Noor 2023)	*Analysis of Top Vulnerabilities in Security of Web-Based Applications*	Studi Keamanan *Web*	Identifikasi kerentanan utama dalam aplikasi *web* dan langkah mitigasi
28	(Matthew Bach-Nutman 2020)	*Understanding The Top* 10 OWASP *Vulnerabilities*	*Literature Review*	Tinjauan mendalam mengenai ancaman OWASP Top 10
29	(Vippalapalli Vikas, T. Meghana, Gundavarapu Kaveri 2023)	*Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website*	Audit Keamanan *Web & Penetration Testing*	Identifikasi kelemahan keamanan *web* dan rekomendasi perbaikan nya
30	Dimas Febriyan Priambodo, Asep Dadan (Rifansyah,	*Penetration Testing Web* XYZ Berdasarkan OWASP *Risk Rating*	OWASP *Risk Rating*	Mengidentifikasi 9 kerentanan keamanan (2 *high,* 1 *medium,* 6 *low*)

	Muhammad Hasbi 2023)			

2.3 Matriks Penelitian

Tabel 2.2 Tabel Matriks Penelitian

No.	Peneliti	Ruang Lingkup																	
		OS			*Framework*					Metode			*Tools*						
		Windows	***Linux***	***MacOS***	***Laravel***	***Express.js***	***Codelgniter***	***Django***	**ASP.NET *Core***	**OWASP *Testing Guide***	***Penetration Testing***	***Dynamic Analysis***	***Burp Suite***	**OWASP ZAP**	**Netcraft**	**SQLmap**	**Metasploit**	**Nmap**	**Netsparker**
1	(Fernanda Tinambunan, Achmad Junaidi, Agung Mustika Rizki 2024 : Pengujian Sistem Informasi Akademik Universitas X Melalui Pendekatan *Penetration Testing* Berdasarkan OWASP Top 1)	-	✓	-	✓	-	-	-	-	✓	✓	-	✓	✓	-	-	-	✓	-
2	(Ichsan Octama Riandhanu 2022 : Analisis Metode *Open Web Application Security Project*	-	✓	-	-	-	✓	-	-	-	✓	-	-	-	-	-	-	-	✓

	(OWASP) Menggunakan *Penetration Testing* pada keamanan *website* absensi)																		
3	(Dimas Febriyan Priambodo, Asep Dadan Firmansyah, Muhammad Hasbi 2023 : *Penetration Testing Web* XYZ Berdasarkan OWASP *Risk Rating*)	✓	-	-	✓	-	-	-	-	✓	-	-	✓	✓	-	-	-	✓	-
4	(Ade Putra Armadhani, Dicky Nofriansyah Khairi Ibnutama 2022 : Analisis Keamanan Untuk Mengetahuai *Vulnerability* Pada DVWA *Lab Testing* Menggunakan *Penetration Testing Standart* OWASP)	-	✓	-	-	-	-	-	✓	-	✓	-	✓	-	-	✓	-	-	-
5	(Ela Nurelasari, Difa Gumilang Al Farabi 2024 : Analisis Keamanan Sistem *Website* Menggunakan Metode *Oen Web Application Security Project* (OWASP) Pada SIMANTEP.ID)	-	✓	-	✓	-	-	-	-	✓	✓	-	-	✓	-	-	-	-	-
6	(Yudiana, Anggi Elanda, Robby Lintang Buana 2021 : Analisis kualitas keamanan sistem informasi *e-office* berbasis *website* pada STIMIK rosma dengan menggunakan OWASP Top 10)	✓	-	-	✓	-	-	-	-	✓	✓	-	-	✓	-	-	-	-	-
7	(Maulana Pandudinata, Farid Ridho 2024 : Analisis kerentanan *website* SMA Negeri 2 Amlapura menggunakan metode OWASP (*open web application security project)*)	✓	-	-	-	-	✓	-	-	-	✓	-	-	✓	-	-	-	-	-

No.	Peneliti	Ruang Lingkup																	
		OS			***Framework***					**Metode**			***Tools***						
		Windows	***Linux***	***MacOS***	***Laravel***	***Express.js***	***Codelgniter***	***Django***	**ASP.NET *Core***	**OWASP *Testing Guide***	***Penetration Testing***	***Dynamic Analysis***	***Burp Suite***	**OWASP ZAP**	**Netcraft**	**SQLmap**	**Metasploit**	**Nmap**	**Netsparker**
8	(Zidan Faizi, Purwantoro, Azhari Ali Ridha 2023 : Analisis Keamanan Aplikasi Berbasis *Web* di Lingkungan BPS RI. Studi Kasus : Aplikasi *Web* Jafung BPS)	-	✓	-	-	-	✓	-	-	-	✓	-	-	✓	✓	-	-	✓	-
9	(Hermawan Setiawan Lytio Enggar Erlangga, Syubbanul Siddiq, Yusuf Atha Gunawan 2023 : Analisis Kerawanan Pada Aplikasi *Website* Menggunakan Standar OWASP Top 10 Untuk penilaian *Risk Rating*)	✓	-	-	-	-	✓	-	-	-	✓	-	-	✓	-	-	-	-	-
10	(Ahmad Alfian Chandra, Ahmad Turmudi Zy, Agung Nugroho 2024 : Penerapan Teknik *Penetration Testing* terhadap *Cross-Site Scripting* (XSS) dalam pengembangan *website*)	✓	-	-	✓	-	-	-	-	✓	✓	-	-	✓	-	-	-	-	-
11	(Urshila Ravindran, Raghu Vamsi Potukuchi 2022 : *A Review on Web Application*	✓	✓	-	✓	-	-	-	-	✓	-	-	-	✓	-	-	-	-	-

	Vulnerability Assessment and Penetreation Testing)																		
12	(Janstipen Roy Mansen Sagala, Yusnia Budiarti, Rosi Kusuma Serli 2024 : Analisis Keamanan Aplikasi *Website* Kecamatan Cibodas Tanggerang Dengan Metode *Open Web Application Security Project*)	-	✓	-	✓	-	-	-	-	✓	✓	-	-	✓	-	-	-	-	-
13	(Bad'ul Hilmi Arromdoni, Mandahadi Kusuma, Bambang Sugiantoro 2024 : *Web Application Vulnerability Analysis Using the* OWASP *Method (Case Study:* OJS CSFD UIN Sunan Kalijaga Yogyakarta)	-	✓	-	-	-	✓	-	-	✓	✓	-	-	✓	-	-	-	-	-
14	(Chinekezi Chinyere Echefunna, Jude Osamor, Celestine Iwendi 2024 : *Evaluation of Information Security in Web Application Through Penetration Testing Techniques Using* OWASP *Risk Methodology)*	✓	✓	-	-	✓	-	-	-	-	✓	-	✓	✓	-	-	-	-	-
15	(Aida Fitriya Sebrina, Achmad Junaidi, Andreas Nugroho Sihananto 2024 : *Testing* Posketanmu *Website with Google Penetration Testing and* OWASP Top 10)	✓	-	-	✓	-	-	-	-	✓	✓	-	✓	✓	-	-	-	✓	-
16	(M. Sakthivel, S. Sivanantham, N. Bharathiraja 2024 : *Ensuring Web Application Security: An* OWASP *Driven Development Methodology*)	✓	-	-	-	-	✓	-	-	✓	-	-	-	✓	-	-	-	-	-
17	(Yoel Armando, Rosalina Rosalina 2023 : *Penetration Testing* Tanggerang *City Web Application With Implementing* OWASP Top 10 *Web Security Risk Framework*)	-	✓	-	-	✓	-	-	-	✓	✓	-	✓	✓	-	✓	-	✓	-

18	(Mistry Mahima Ankit 2024 : *Unveling the Underbelly of Web Application Vulnerabilities: A critical Exploration*)	✓	✓	-	-	✓	-	-	-	✓	✓	-	✓	-	-	✓	-	✓	-
19	(Yuvraj Singh 2024 : *WebSec: Exploring and Modulating Vulnerabilities*)	-	✓	-	-	-	-	✓	-	✓	✓	-	✓	-	-	✓	-	✓	-
20	(Madhuri N. Gedam, Bandu B. Meshram 2023 : *Web Application Top* 10 OWASP *Attacks and Defence Mechanism*)	✓	-	-	-	-	-	✓	-	✓	✓	-	-	-	-	✓	-	-	-
21	(Malak Saleh Aljabri, Maryam AlDossary, Noor Al-Homeed 2022 : *Testing and Exploiting Tools to Improve* OWASP *Top Ten Security Vulnerabilities Detection*)	-	✓	-	✓	-	-	-	-	✓	✓	-	✓	✓	-	✓	-	-	-
22	(Sonali Patil, Mandaar Rao, Lavitra Misal 2023 : *A Review of the* OWASP Top 10 *Web Application Security Risks and Best Practices for Mitigating These Risks*)	✓	-	-	✓	-	-	-	-	✓	-	-	✓	✓	-	-	-	-	-
23	(Muhamad Agreinda Helmiawan, Esa Firmansyah, Irfan Fadil 2020 : *Analysis of Web Security Using Open Web Application Security Project* 10)	-	✓	-	-	✓	-	-	-	✓	-	-	-	✓	-	-	-	✓	-
24	(E. Altulaihan, Abrar Alismail, Mounir Frikha 2023 : *A Survey on Web Application Penetration Testing*)	✓	-	-	✓	-	-	-	-	-	✓	-	✓	-	-	✓	-	✓	-
25	(Petar T. Lachkov, Lo'ai Tawalbeh, Smriti Bhatt 2022 : *Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing*)	-	✓	-	-	-	✓	-	-	-	✓	-	✓	-	✓	✓	-	-	✓

26	(Ravinder Singh, Manan Gupta, Dipak Raghunath Patil 2024 : *Analysis of Web Application Vulnerabilities using Dynamic Application Security Testing*)	✓	-	-	-	-	-	✓	-	-	-	✓	-	-	✓	✓	-	-	-
27	(Jyoti Rawat, Indrajeet Kumar, Mohd Halim, Mohd Noor 2023 : *Analysis of Top Vulnerabilities in Security of Web-Based Applications*)	✓	-	-	✓	-	-	-	-	-	-	✓	✓	✓	-	-	-	✓	-
28	(Matthew Bach-Nutman 2020 : *Understanding The Top* 10 OWASP *Vulnerabilities*)	-	✓	-	-	✓	-	-	-	✓	-	-	-	✓	-	-	-	✓	-
29	(Vippalapalli Vikas, T. Meghana, Gundavarapu Kaveri 2023 : *Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website*)	-	✓	-	✓	-	-	-	-	-	✓	-	✓	-	-	-	-	✓	-
30	Dimas Febriyan Priambodo, Asep Dadan (Rifansyah, Muhammad Hasbi 2023 : *Penetration Testing Web* XYZ Berdasarkan OWASP *Risk Rating*)	✓	✓	-	✓	-	-	-	-	-	✓	✓	-	✓	✓	✓	-	✓	-
31	(Usulan Penelitian : Analisis Keamanan Aplikasi *Web* Menggunakan *Web Application Penetration Testing* Berdasarkan OWASP Top 10	✓	✓	-	✓	-	-	-	-	✓	✓	-	✓	✓	-	✓	-	✓	-

2.4 *Research Gap*

Berdasarkan tinjauan terhadap penelitian-penelitian terdahulu mengenai pengujian keamanan aplikasi berbasis OWASP Top 10, mayoritas penelitian fokus pada pemindaian otomatis menggunakan *velnerability scanner* (OWAS ZAP atau Acunetix) tanpa melakukan pembuktian mendalam *(Proof of Concept)* terhadap status *True Positive* maupun *Negative Finding.* Selain itu, sebagian besar studi terdahulu tidak menyajikan evaluasi risiko secara kuantitatif serta belum memetakan kerentanan ke dalam standar pengujian *Web Security Testing Guide* (WSTG).

2.5 Kebaruan dan Kontribusi Penelitian

Kebaruan *(novelty)* dan kontribusi penelitian ini terletak pada penerapan kerangka kerja OWASP WSTG yang dipadukan dengan perhitungan skor risiko kuantitatif, Pembuktian eksploitasi manual terkendali, serta penyusunan matriks manajemen risiko yang aplikatif untuk sistem informasi akademik SINTESYS Universitas Siliwangi