SYSTEMATIC LITERATURE REVIEW PENETRATION TESTING PADA KEAMANAN WEBSITE

Lamintang Ramadhan[1], Nurul Maharani Piranti[2], Okky Pratama Martadireja[3]
[1,2,3] Politeknik Imigrasi,
lamintangr1234@gmail.com[1] , nurulpiranti20@gmail.com[2], okkypm@gmail.com[3]

ABSTRACT

Advances in internet technology pose major challenges in maintaining website security against various cyber threats. This Systematic Literature Review (SLR) aims to identify and analyze the methods and tools used in website security testing with a focus on penetration testing. This study was conducted by screening 1,911,363 initial articles obtained from various academic repositories, such as IEEE Xplore, Springer Link, Crossref, Semantic, and Google Scholar, resulting in 32 articles that met the inclusion criteria based on their relevance and quality. The results of the study show that the penetration testing approach is dominated by various security frameworks, including OWASP, ISSAF, OSSTMM, and PTES, which are used to evaluate and strengthen web system security. In addition, this study reveals that tools such as Acunetix, Nmap, Metasploit, Burp Suite, and SQLmap are often used to detect and exploit security vulnerabilities. Several studies also highlight the integration of machine learning technology in detecting attacks such as SQL Injection and Cross-Site Scripting (XSS), which indicates a new trend in website security testing. The conclusion of this study emphasizes the need for a more adaptive approach to penetration testing, combining automation techniques and manual analysis to improve the effectiveness of threat detection and mitigation. The results of this study can serve as a reference for academics and cybersecurity practitioners in choosing the optimal strategy to secure website systems from evolving threats.

Keywords: cybersecurity , *literature review*, *OWASP, penetration testing*

ABSTRAK

Kemajuan teknologi internet membawa tantangan besar dalam menjaga keamanan website dari berbagai ancaman siber. Systematic Literature Review (SLR) ini bertujuan untuk mengidentifikasi dan menganalisis metode serta alat yang digunakan dalam pengujian keamanan website dengan fokus pada penetration testing. Penelitian ini dilakukan dengan menyaring 1.911.363 artikel awal yang diperoleh dari berbagai repositori akademik, seperti IEEE Xplore, Springer Link, Crossref, Semantic, dan Google Scholar, hingga menghasilkan 32 artikel yang memenuhi kriteria inklusi berdasarkan relevansi dan kualitasnya. Hasil kajian menunjukkan bahwa pendekatan penetration testing didominasi oleh berbagai framework keamanan, termasuk OWASP, ISSAF, OSSTMM, dan PTES, yang

digunakan untuk mengevaluasi dan memperkuat keamanan sistem web. Selain itu, penelitian ini mengungkap bahwa alat seperti Acunetix, Nmap, Metasploit, Burp Suite, dan SQLmap sering digunakan dalam mendeteksi serta mengeksploitasi kerentanan keamanan. Beberapa studi juga menyoroti integrasi teknologi machine learning dalam mendeteksi serangan seperti SQL Injection dan Cross-Site Scripting (XSS), yang menunjukkan tren baru dalam pengujian keamanan website. Kesimpulan dari studi ini menekankan perlunya pendekatan yang lebih adaptif dalam penetration testing, dengan kombinasi teknik otomatisasi dan analisis manual untuk meningkatkan efektivitas deteksi serta mitigasi ancaman. Hasil dari penelitian ini dapat menjadi referensi bagi akademisi dan praktisi keamanan siber dalam memilih strategi yang optimal untuk mengamankan sistem website dari ancaman yang terus berkembang.

Kata Kunci: *cybersecurity* , keamanan website, *literature review*, *owasp, penetration testing*

A. Pendahuluan

Keamanan website merupakan aspek krusial dalam era digital yang semakin berkembang pesat. Dengan meningkatnya ketergantungan pada layanan berbasis web, risiko terhadap serangan siber juga semakin meningkat. Serangan seperti SQL Injection (SQLi), Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS), dan Man-in-the-Middle (MitM) menjadi ancaman serius yang dapat mengeksploitasi kelemahan sistem dan mengakibatkan kebocoran data, manipulasi informasi, hingga gangguan layanan yang signifikan. Oleh karena itu, metode pengujian keamanan seperti penetration testing dan vulnerability assessment menjadi bagian esensial dalam strategi pertahanan siber.

Salah satu metode yang banyak digunakan dalam pengujian keamanan website adalah penetration testing, yang bertujuan untuk mengidentifikasi celah keamanan dengan mensimulasikan serangan yang mungkin terjadi. Seiring berkembangnya ancaman siber, berbagai framework dan alat bantu telah dikembangkan untuk meningkatkan efektivitas pengujian ini, termasuk OWASP, ISSAF, OSSTMM, dan PTES, serta perangkat lunak seperti Acunetix, Burp Suite, Nmap, SQLmap, dan Metasploit. Untuk memahami tren terbaru dalam pengujian keamanan website, penelitian ini menggunakan pendekatan Systematic Literature Review (SLR). SLR merupakan metode penelitian yang digunakan

untuk mengumpulkan, mengevaluasi, dan mensintesis penelitian yang relevan secara sistematis, dengan tujuan memberikan wawasan menyeluruh terhadap suatu topik penelitian. Dalam studi ini, dilakukan analisis terhadap artikel yang diperoleh dari berbagai basis data akademik, termasuk IEEE Xplore, Springer Link, Crossref, Semantic, dan Google Scholar, dengan periode publikasi antara 2015 hingga 2025.

Penelitian ini bertujuan untuk menjawab dua pertanyaan utama:

1. Bagaimana karakteristik utama dalam pengujian keamanan website?
2. Apa metode dan alat yang paling banyak digunakan dalam pengujian keamanan website?

Hasil penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai teknik penetration testing, framework yang digunakan, serta tantangan dan peluang dalam meningkatkan keamanan website. Dengan demikian, penelitian ini dapat menjadi referensi bagi akademisi dan praktisi dalam memilih strategi terbaik untuk mengamankan sistem website dari ancaman siber yang semakin kompleks.

B. Metodologi Penelitian

Tahap 1 : Kriteria Kelayakan Artikel

Kriteria kelayakan artikel ditentukan oleh Inclusion Criteria (IC), yaitu:

a. IC1: Artikel harus merupakan penelitian asli yang telah dipublikasikan dalam bahasa Inggris atau Indonesia serta tersedia dalam jurnal akademik atau konferensi bereputasi.

b. IC2: Artikel diterbitkan antara tahun 2015 hingga 2025 guna memastikan informasi terkini mengenai pengujian keamanan website

c. IC3: Artikel bertujuan untuk menganalisis metode dan framework keamanan siber, terutama dalam konteks pengujian keamanan website berbasis penetration testing, risk assessment, atau vulnerability assessment.

Tahap 2 : Penetapan Sumber Artikel

Literatur dicari dalam basis data akademik dengan repositori signifikan untuk studi keamanan siber, seperti Semantic, IEEE Xplore, Crossref, Springer Link, dan Google Scholar.

Pada artikel yang memenuhi Inclusion Criteria (IC), penelitian terkait juga dieksplorasi menggunakan teknik backward snowballing, yaitu dengan

meninjau referensi dalam studi yang relevan, serta forward snowballing untuk menemukan studi yang mengutip artikel tersebut.

Tahap 3 : Pemilihan Literatur

Kata kunci utama yang digunakan dalam pencarian adalah:

Website security

Website Penetration Test

Artikel yang diperoleh diseleksi berdasarkan judul dan abstrak, untuk memastikan keterkaitannya dengan pertanyaan penelitian (Research Questions - RQ).

Artikel yang telah lolos tahap awal akan dibaca secara penuh atau sebagian untuk menentukan apakah memenuhi kriteria peninjauan lanjutan.

Jika dalam artikel terdapat metode atau teknik tambahan selain Website Penetration Test, penelitian tersebut tetap dapat dimasukkan jika memiliki relevansi tinggi dengan pengujian keamanan website

Tahap 4 : Pengumpulan Data

Data dikumpulkan secara sistematis dengan menggunakan formulir ekstraksi data yang mencakup informasi seperti : Judul penelitian,Tahun publikasi,Metodologi yang digunakan (Penetration Test, kombinasi dengan framework lain),Temuan utama (efektivitas framework, metrik evaluasi, integrasi dengan metode lain),Kontribusi terhadap bidang keamanan siber Penelitian ini memfilter jumlah awal jurnal yang ditemukan berdasarkan kata kunci yang telah ditentukan. Setelah dilakukan penyaringan berdasarkan judul, abstrak, dan metodologi, hanya artikel yang berkualitas tinggi dan relevan yang akan dianalisis lebih lanjut. Sebagai contoh, dari 1.911.363 jurnal yang diperoleh dalam pencarian awal, hanya 103 artikel yang memenuhi syarat untuk peninjauan lebih dalam, dan setelah proses seleksi lanjutan, 32 jurnal terpilih digunakan sebagai referensi utama dalam penelitian ini.

Tabel 1 Hasil Pencarian Jurnal

Sumber	Website security	Website Penetration Test	Kandidat	Terpilih
Link Springer	108.925	10.304	5	0
IEEE Xplore	4.484	136	5	1
Crossref	680.054	782,021	31	8
Semantic	1.100.000	121.000	23	4
Google Scholar	17.900	28.000	39	19
Total	**1.911.363**	**941.461**	**103**	**32**

Tabel 2 *Research Question*

ID	Pertanyaan Penelitian	Latar Belakang
RQ 1	Bagaimana karakteristik utama dalam pengujian keamanan website?	Mengidentifikasi karakteristik utama dalam pengujian keamanan website
RQ 2	Apa metode dan alat yang paling banyak digunakan dalam pengujian keamanan website ?	Mengidentifikasikan metode yang paling efektif dalam mengidentifikasi dan mengevaluasi celah keamanan pada website

C. Hasil dan Pembahasan

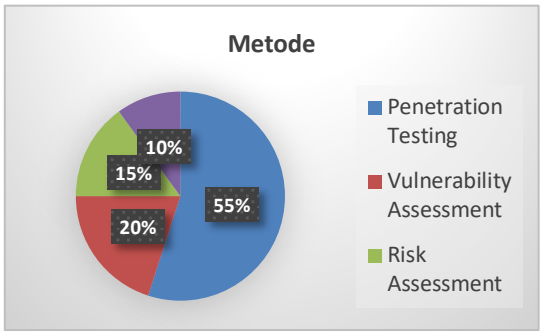
Tabel 3 Daftar Jurnal Terkait

No.	Judul	Tahun	Metode	Platform	Tools
1	Beyond the west…[1]	2025	leveraging various detection methods	Website	ML-PWD, LaSeTo
2	Implementasi Secure..[2]	2025	Penetration Testing	Website	OWASP ZAP
3	Pengujian Keamanan…[3]	2025	Penetration Testing	Website	Acunetix
4	Analisis dan Rekom..[4]	2025	ISSAF	Website	Owasp Zap Top 10, Nmap, Acunetix
5	Evaluasi Celah..[5]	2024	ISSAF	Website	Owasp Zap Top 10, Nmap, Acunetix
6	Improving the..[6]	2024	SQL injection	Website	SQL-Map
7	INFORMATION TECH..[7]	2024	ISSAF , ISO 31000	Website	Whois Domain, Netcraft, NMAP
8	Web Application….[8]	2024	ISSAF, 0SSTMM	Website	Google Search Engine, HAProxy load Balancer, Nmap, Nikto
9	Penetration Tes..[9]	2023	Blaxbox	Website	OWASP 10, Nmap, Dirb, Nikto
10	Impact Analysis…[10]	2023	Experimental Method, WAF testing	Website	OWASP , Remote VPS
11	Analisis Celah..[11]	2023	Penetration Testing, ISSAF	Website	Kali Linux, Virtual Box, OWASP ZAP
12	Website Security…[12]	2023	Vulnerability Assessment	Website	OWASP ZAP , Acunetix, Vega, OpenVAS
13	A Survey…[13]	2023	Manual Penetration Testing, Automated Penetration Testing	Website	OWASP Top 10 Web, SCANSCX, NMAP, Wireshark, Metasploit, ,Burp Suite.
14	Detection of cros…[14]	2023	Machine learning techniques, XSS attack	Website	OWASP, Q-Learning, Q net- works
15	Security Vulnerability..[15]	2023	Penetration Testing	Website	OWASP ZAP, Acunetix, Nmap, Paros
16	Analysis and…[16]	2023	ISSAF, OSSTMM	Website	WPScan, LOIC, Nmap
17	Analisis Keamanan…[17]	2023	ISSAF	Website	OWASP, Nmap, Acunetix
18	Pentesting on..[18]	2023	Penetration Testing, OSSTMM, ISSAF	Website	Burp Suite, SQLmap, What Web, Nessus Nessus
19	Techniques For Tes…[19]	2022	Escaping Metacharacter	Website	NMAP, Kali linux
20	Analysis of Open…[20]	2022	OWASP, ISSAF	Website	Whois Domain, Nmap, Acunetix, Zenmap, SQLmap
21	Evaluasi Risiko…[21]	2022	OSSTMM	Website	Nmap, Nessus, Whois, Wireshark
22	Pengujian Keren…[22]	2021	Penetration Testing	Website	WPScan,
23	Web application….[23]	2021	Penetration Testing	Website	OWASP,
24	Web Vulnerability..[24]	2021	Web Vulnerability	Website	OWASP Security Shepherd
25	Testing for Sec…[25]	2020	Ethical Hacking	Website	OWASP's Zed, Netcraft, Sparta
26	Evaluasi Keamanan..[26]	2020	ISSAF	Website	Whois Domain, Nmap, IP lookup Scanner, Vega, Owaspzap
27	Information tech..[27]	2020	ISO 31000, ISSAF	Website	Whois Domain, Spamhaus, Spamcom, Netcraft, NMap
28	Cross-site scri…[28]	2020	Cross-Site Scripting (XSS) Attacks	Website	OWASP Top 10
29	Vulnerability Ass…[29]	2019	Vulnerability Assessment and Penetration Testing (VAPT)	Website	OWASP Top 10
30	Penetration testing..[30]	2019	Penetration Testing	Website	Kali Linux, Metasploit, Wireshark, John The Ripper, Nessus, Nmap, Dradis

31	Vulnerability Asses…[31]	2019	Vulnerability Assessment, Penetration Testing
32	Web appli…[32]	2019	Penetration Testing, OWASP top 10

Keamanan website telah menjadi fokus utama dalam bidang cybersecurity, seiring dengan meningkatnya ancaman siber yang menargetkan aplikasi web. Berdasarkan analisis terhadap berbagai jurnal yang memenuhi kriteria seleksi, tren penelitian dalam penetration testing menunjukkan peningkatan signifikan dalam beberapa tahun terakhir. Studi oleh Kholiq (2017) mengindikasikan bahwa penetration testing merupakan metode efektif untuk mensimulasikan teknik yang mungkin digunakan oleh penyerang untuk mengakses sistem secara ilegal

Selain itu, penelitian oleh Hernawan dan Kho (2019) menekankan pentingnya penetration testing dalam mengidentifikasi dan mengatasi kerentanan pada sistem sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab Hal ini menunjukkan urgensi dalam mengembangkan metode pengujian keamanan yang adaptif dan efektif untuk melindungi aplikasi web dari berbagai ancaman siber. Dari hasil analisis, ditemukan bahwa metode utama yang digunakan dalam pengujian keamanan website meliputi:
Penetration Testing (55%) – Teknik eksplorasi aktif yang bertujuan mengidentifikasi serta mengeksploitasi celah keamanan yang ada dalam sistem website.
Vulnerability Assessment (20%) – Pendekatan yang berfokus pada identifikasi dan evaluasi potensi kerentanan tanpa eksploitasi langsung.
Risk Assessment (15%) – Metode berbasis manajemen risiko untuk mengukur tingkat ancaman serta dampaknya terhadap keamanan website.



Gambar 1 . Diagram persentase metode yang digunakan dalam *penetration testing*

Menurut Kholiq (2017), penetration testing memungkinkan simulasi metode yang mungkin digunakan oleh penyerang untuk

menghindari atau menerobos mekanisme keamanan dan mendapatkan akses ilegal ke dalam sistem

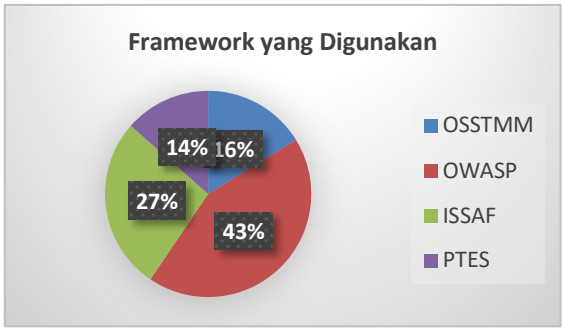
Hal ini sejalan dengan penelitian Hernawan dan Kho (2019) yang menyatakan bahwa penetration testing adalah cara efektif untuk mengidentifikasi dan mengatasi kerentanan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab Dalam proses penetration testing, berbagai framework dan tools digunakan untuk menguji serta mengevaluasi keamanan website. Beberapa framework yang paling sering digunakan meliputi:

a. OWASP (Open Web Application Security Project) – 43% Framework ini menyediakan standar pengujian keamanan web, termasuk daftar OWASP Top 10, yang berisi jenis serangan paling umum terhadap aplikasi web.

b. ISSAF (Information Systems Security Assessment Framework) – 27% Framework ini memberikan panduan dalam melakukan penetration testing secara sistematis dan terstruktur.

c. OSSTMM (Open Source Security Testing Methodology Manual) – 16% Metode ini lebih berfokus pada standar keamanan berbasis praktik pengujian keamanan terbuka.

d. PTES (Penetration Testing Execution Standard) – 14% Standar ini menyediakan tahapan lengkap dalam penetration testing, mulai dari perencanaan hingga analisis hasil eksploitasi.



Gambar 2 . Diagram persentase *framework* yang digunakan dalam *penetration testing*

Menurut Darmayuda et al. (2021), penggunaan framework seperti ISSAF dalam penetration testing membantu dalam mengidentifikasi serangan yang mungkin terjadi terhadap kerentanan yang ada pada sistem, serta memahami dampak bisnis yang diakibatkan dari eksploitasi yang dilakukan oleh penyerang

Selain framework, berbagai tools digunakan untuk mendukung proses penetration testing. Beberapa alat yang paling umum digunakan meliputi:

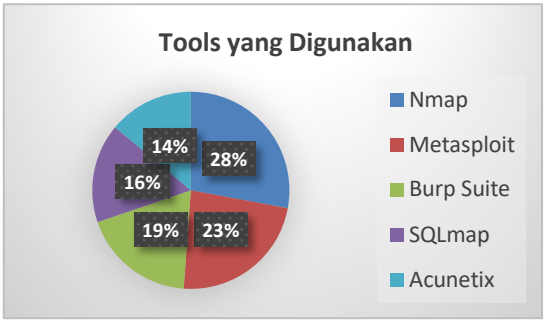
a. Nmap (28%) – Untuk scanning jaringan dan deteksi layanan yang berjalan.

b. Metasploit (23%) – Untuk eksploitasi otomatis terhadap celah keamanan.

c. Burp Suite (19%) – Untuk analisis keamanan aplikasi web.

d. SQLmap (16%) – Untuk mendeteksi dan mengeksploitasi SQL Injection.

e. Acunetix (14%) – Untuk pemindaian kerentanan otomatis pada website.



Gambar 3. Diagram persentase *tools* yang digunakan dalam *penetration testing*

Penggunaan tools ini memungkinkan pengujian yang lebih mendalam dan sistematis terhadap keamanan aplikasi web, sehingga potensi kerentanan dapat diidentifikasi dan ditangani sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab.

D. Kesimpulan

Dalam kajian ini, ditemukan bahwa penetration testing merupakan salah satu metode paling efektif dalam mengidentifikasi dan mengeksploitasi celah keamanan pada sistem website. Pendekatan ini memungkinkan simulasi serangan yang dapat digunakan oleh peretas untuk menembus sistem keamanan. Dengan demikian, metode ini menjadi langkah preventif yang sangat penting dalam menjaga keamanan aplikasi web dari ancaman siber yang terus berkembang. Berbagai framework seperti OWASP, ISSAF, OSSTMM, dan PTES digunakan untuk memastikan pengujian yang sistematis, sementara alat bantu seperti Nmap, Metasploit, Burp Suite, dan SQLmap membantu mendeteksi serta mengeksploitasi kerentanan. Tren terbaru menunjukkan bahwa teknologi machine learning mulai diterapkan untuk meningkatkan akurasi deteksi serangan, khususnya terhadap ancaman seperti SQL Injection dan Cross-Site Scripting (XSS).

Untuk meningkatkan keamanan website, diperlukan pendekatan yang adaptif dengan mengombinasikan teknik manual dan otomatis dalam

penetration testing. Penggunaan framework standar harus dioptimalkan agar pengujian lebih sistematis, sementara teknologi machine learning dapat dimanfaatkan untuk mempercepat deteksi ancaman. Selain itu, pelatihan berkala bagi pengembang dan praktisi keamanan siber sangat diperlukan agar selalu mengikuti perkembangan teknik terbaru. Yang tak kalah penting, penetration testing harus menjadi bagian dari kebijakan keamanan organisasi secara menyeluruh agar mitigasi ancaman dapat dilakukan lebih proaktif dan efektif.

DAFTAR PUSTAKA

Yuan, Y., Apruzzese, G., & Conti, M. (2025). Beyond the west: Revealing and bridging the gap between Western and Chinese phishing website detection. Computers & Security, 148(June 2024), 104115. https://doi.org/10.1016/j.cose.2024.104115

Ariyadi, T., Salsabila, A. P., & Nugroho, Y. P. (2025). Implementasi secure code pada pengembangan sistem keamanan website Teknik Komputer Universitas Bina Darma menggunakan penetration testing dan OWASP ZAP. Jurnal, 4(1).

Ainurrohman, M., & Nurasri, Y. (2025). Pengujian keamanan website JDIH Kab. Tegal menggunakan Acunetix dengan standar ISO/IEC 27001:2013. Jurnal, 2(3), 3320–3323.

Issaf, M. (2025). Analisis dan rekomendasi keamanan website Kampus X. Jurnal, 6(1), 830–843.

Mario, F., Tjiptabudi, H., & Ndaumanu, R. I. (2024). Evaluasi celah keamanan website Dana Pensiun X melalui penetration testing berdasarkan ISSAF framework. Algoritma, 21(2), 9–17. https://doi.org/10.33364/algoritma/v.21-2.1644

Huovila, V. (2024). Improving the security of SQL Server using SQL-Map tool. Jurnal, (February).

Perdianza, M. E., Firdaus, M. A., Indah, D. R., Sriwijaya, U., Ilir, O., & Selatan, S. (2024). Information technology risk management using ISO 31000 based on the ISSAF penetration testing framework. Jurnal, 839–851.

Agung, I. G., & Pramana, S. (2024). Web application penetration testing on Udayana University's OASE E-learning platform using Information System Security Assessment Framework (ISSAF) and Open Source Security Testing Methodology Manual (OSSTMM). International Journal of Information Technology and Computer Science, 16(2), 45–56.

https://doi.org/10.5815/ijitcs.2024.02.04

Jaelani, W. L., Yanto, Y., & Khoirunnisa, F. (2023). Penetration testing website dengan metode black box testing untuk meningkatkan keamanan website pada instansi. Naratif: Jurnal Nasional Riset, Aplikasi, dan Teknologi Informasi, 5(1), 1–8. https://doi.org/10.53580/naratif.v5i1.180

Pratama, K. D., & Anwar, N. (2023). Impact analysis of web application firewall on website-based application security (Case study PPDB Kak Seto School Website). Mobile Forensics, 5(1), 44–58. https://doi.org/10.12928/mf.v5i1.8914

Andriyani, S., Sidiq, M. F., & Zen, B. P. (2023). Analisis celah keamanan pada website dengan menggunakan metode penetration testing dan framework ISSAF pada website SMK Al-Kautsar. Jurnal Informatika dan Information Technology, 8798, 1–13.

Adha, M., KWA, Z. D., & Muhammad, A. H. (2023). Website security test at the University of Mataram using vulnerability assessment. JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), 8(2), 647–655. https://doi.org/10.29100/jipi.v8i2.3830

Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). A survey on web application penetration testing. Electronics, 12(5). https://doi.org/10.3390/electronics12051229

Kaur, J., Garg, U., & Bathla, G. (2023). Detection of cross-site scripting (XSS) attacks using machine learning techniques: A review. Artificial Intelligence Review, 56(11). https://doi.org/10.1007/s10462-023-10433-3

Safitra, M. F., Lubis, M., & Widjajarto, A. (2023). Security vulnerability analysis using Penetration Testing Execution Standard (PTES): Case study of government's website. ACM International Conference Proceeding Series, 139–145. https://doi.org/10.1145/3592307.3592329

Nabila, A., Mas, E., & Saptono, R. (2023). Analysis and implementation of the ISSAF framework on OSSTMM on website security vulnerabilities testing in Polinema. Jurnal, 13(1).

Fitri, I. N. (2023). Analisis keamanan website. Fakultas Teknik dan Sains, UMP.

Shaik, A. (2023). Pentesting on web applications using ethical hacking. Gannon University.

Utama, A. W., & Fitrani, A. S. (2022). Techniques for testing website

security using the escaping metacharacter method. Procedia Engineering and Life Science, 2(2). https://doi.org/10.21070/pels.v2i2.1223

Ashar, R. (2022). Analysis of open website security using OWASP and ISSAF methods. Jurnal Informasi dan Teknologi, 4(4), 187–194. https://doi.org/10.37034/jidt.v4i4.233

Ilmi, A., Seta, H. B., & Pradnyana, I. W. W. (2022). Evaluasi risiko celah keamanan menggunakan metodologi Open-Source Security Testing Methodology Manual (OSSTMM) pada aplikasi web terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta. Jurnal, 4221, 190–197.

Azis, R., & Yazid, S. (2021). Pengujian kerentanan website Wordpress dengan menggunakan penetration testing untuk menghasilkan website yang aman. Jurnal Restikom: Riset Teknik Informatika dan Komputer, 3(3), 93–105.

Alanda, A., Satria, D., Ardhana, M. I., Dahlan, A. A., & Mooduto, H. A. (2021). Web application penetration testing using SQL injection attack. International Journal of Informatics and Visualization, 5(3), 320–326. https://doi.org/10.30630/joiv.5.3.470

Wibowo, R. M., & Sulaksono, A. (2021). Web vulnerability through cross site scripting (XSS) detection with OWASP Security Shepherd. Indonesian Journal of Information Systems, 3(2), 149–159. https://doi.org/10.24002/ijis.v3i2.4192

Devi, R. S., & Kumar, M. M. (2020). Testing for security weakness of web applications using ethical hacking. Proceedings of the 4th International Conference on Trends in Electronics and Informatics (ICOEI 2020), 354–361. https://doi.org/10.1109/ICOEI48184.2020.9143018

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi keamanan website Lembaga X melalui penetration testing menggunakan framework ISSAF. Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi), 8(2), 113. https://doi.org/10.24843/jim.2020.v08.i02.p05

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Information technology risk management using ISO 31000 based on ISSAF framework penetration testing (Case study: Election commission of X city). International Journal of Computer Networks and Information Security, 12(4), 30–40. https://doi.org/10.5815/ijcnis.2020.04.03

Rodríguez, G. E., Torres, J. G., Flores, P., & Benavides, D. E. (2020). Cross-site scripting (XSS) attacks

and mitigation: A survey. Computer Networks, 166(November). https://doi.org/10.1016/j.comnet.2019.106960

Simran, G., & D, S. (2019). Vulnerability assessment of web applications using penetration testing. International Journal of Recent Technology and Engineering, 8(4), 1552–1556. https://doi.org/10.35940/ijrte.b2133.118419

Sahiti, V., Tilakchand, P., Kowshik, B., Avinash, P., & Kavya, S. L. (2019). Penetration testing using Wireshark and defensive mechanisms against MITM. International Journal of Recent Technology and Engineering, 7(6), 880–885.

Goutam, A., & Tiwari, V. (2019). Vulnerability assessment and penetration testing to enhance the security of web application. Proceedings of the 4th International Conference on Information Systems and Computer Networks (ISCON 2019), 601–605. https://doi.org/10.1109/ISCON47742.2019.9036175

Nagendran, K., Adithyan, A., Chethana, R., Camillus, P., & Varshini, K. B. B. S. (2019). Web application penetration testing. International Journal of Innovative Technology and Exploring Engineering, 8(10), 1029–1035. https://doi.org/10.35940/ijitee.J9173.0881019,