VOL. 10. NO. 2 NOVEMBER 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480 /jitk.v10i2.5534

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

APPLICATION OF OWASP ZAP FRAMEWORK FOR SECURITY ANALYSIS OF LMS USING PENTEST METHOD

Rusydi Umar[1]; Imam Riadi[2]; Sonny Abriantoro Wicaksono[3*]

Master Program of Informatics[1,3]
Information System[2]
Universitas Ahmad Dahlan Yogyakarta, Indonesia[1,2,3]
https://uad.ac.id/[1,2,3]
rusydi@mti.uad.ac.id[1], imam.riadi@is.uad.ac.id[2], sonny2008048044@webmail.uad.ac.id[3*]

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

Abstract—*Learning Management System (LMS) is an application currently popular for online learning. The presence of LMS offers better prospects for the world of education, where its highly efficient use allows learning anywhere and anytime through the internet or other computer media. This study focuses on analyzing the security of the Learning Management System (LMS) on the domain e-learning.ibm.ac.id using the Pentest method with the Owasp Zap Framework. Security is a crucial step that needs to be considered by IBM Bekasi in protecting data and information from hacker threats. In this study, the method used is Pentest. Pentest is a series of methods used to test the security of a system by conducting literature studies, searching for data information, and domain information, followed by testing using Owasp Zap to find security-related vulnerabilities. The results of the testing using the Pentest method involve several stages of testing and scanning. The first step is checking domain information using Whois Lookup tools and then scanning using ZenMap on e-learning.ibm.ac.id. In this domain information search, the domain status serverTransferProhibited and clientTransferProhibited was found. The next stage is Vulnerability Analysis, where scanning is performed on the domain e-learning.ibm.ac.id using Owasp Zap tools. Based on the results from Owasp Zap scan, 16 vulnerabilities were found, with the breakdown being 2 high risk, 3 medium risk, 6 low risk, and 5 informational. In the exploitation stage using SQLMap, errors were found in the tested parameters, preventing injection.*

Keywords: *LMS, owasp zap, pentest, security.*

Intisari—*Learning Management System (LMS) adalah aplikasi yang saat ini populer digunakan untuk pembelajaran online. Kehadiran LMS menawarkan harapan yang lebih baik bagi dunia Pendidikan, di mana penggunaannya yang sangat efisien memungkinkan pembelajaran di mana saja dan kapan saja melalui internet atau media komputer lainnya. Studi ini berfokus menganalisis keamanan Learning Management System (LMS) pada domain e-learning.ibm.ac.id menggunakan metode Pentest dengan Framework Owasp Zap. Dimana keamanan merupakan suatu langkah penting yang perlu diperhatikan oleh pihak IBM Bekasi dalam melindungi data dan informasi dari ancaman peretas. Pada penelitian ini metode yang digunakan adalah Pentest, Pentest adalah serangkaian metode yang digunakan untuk menguji keamanan suatu sistem dengan studi literatur, mencari informasi data, dan informasi domain, yang selanjutnya dilakukan pengujian menggunakan Owasp Zap untuk mencari celah terkait keamanan. Hasil pengujian menggunakan metode pentest dengan beberapa tahap pengujian dan scanning dengan langkah pertama melakukan pengecekan informasi domain menggunakan tools whois domain dan dilanjutkan dengan melakukan scanning menggunakan ZenMap pada e-learning.ibm.ac.id, pada pencarian informasi domain ini dihasilkan status domain serverTransferProhibited dan clientTransferProhibited. Tahap selanjutnya adalah Vulnerability Analysis, dimana pada tahap ini melakukan scanning pada domain e-learning.ibm.ac.id menggunakan tools Owasp Zap. Berdasarkan hasil pemindaian Owasp Zap ditemukan 16 kerentanan dengan rincian 2 tingkat risiko high, 3 dengan tingkat risiko medium, 6 kerentanan dengan tingkat risiko low, dan 5 bersifat*

VOL. 10. NO. 2 NOVEMBER 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i2.5534

informasional. Dan pada tahap exploitation menggunakan SQLMap, dapat dihasilkan adanya eror pada parameter yang diuji sehingga tidak dapat dilakukan injeksi.

***Kata Kunci**: LMS, owasp zap, pentest, keamanan.*

INTRODUCTION

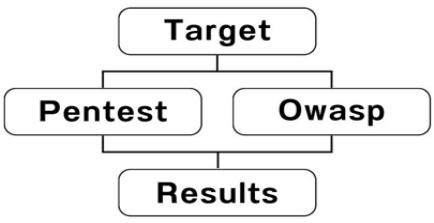
In the current era of globalization, advancements in Information Technology have progressed so rapidly that their usage can be more effective [1]. Information technology has transformational potential across various fields [2]. One of the developments that can be felt is mobile and web-based applications, where this development is considered to facilitate implementation in all fields [3]. One of them is in the field of education, where currently technology brings about a very central change in education [4]. Currently, Information and Communication Technology offers various platforms for teaching activities known as LMS/E-Learning, which can be conducted online remotely, enabling learners to be independent, proficient, and innovative in their learning [5]. The presence of Learning Management Systems (LMS) strengthens the learning process, where currently Learning Management System (LMS) is no longer an option but a necessity. The presence of Learning Management System (LMS) creates an engaging learning environment, enabling students to maintain their autonomy, enthusiasm, and motivation through its use [6].

As an important and efficient technology, security is a key factor that must be considered. Vulnerabilities in security can provide opportunities for unauthorized parties to access [7]. The advancement of this technology has resulted in an increase in cybercrime [8]. Cybersecurity has had a significant impact on the field of education, where several researchers are developing new techniques to enhance the security of systems in this educational field [9]. Cybersecurity plays a crucial role in the educational context, addressing issues such as data theft, account hacking, ransomware attacks, loss of data integrity, and service disruptions. Based on this background, the researcher analyzes and identifies security vulnerabilities in the Learning Management System (LMS) at Muhammadiyah Institute of Business Bekasi with the domain e-learning.ibm.ac.id, aiming to understand potential security threats that could enable external parties to conduct hacking. Furthermore, the goal of this research is to provide insights and recommendations to strengthen system security, thereby protecting the system from potential cyber attacks [10].

In this research, the OWASP approach is used with the Zed Attack Proxy (ZAP) tool and employing the Pentest method. OWASP is an open framework capable of enhancing system security [11]. OWASP ZAP is a great tool for testing someone conducting testing on the system they own [12]. With OWASP ZAP, various issues related to SQL Injection, Broken Authentication, Sensitive Data Exposure, Broken Access Control, Security Misconfiguration, and Cross Site Scripting (XSS) can be detected [13]. As a tool designed for penetration testing, OWASP ZAP is an ideal choice for vulnerability scanning methods [14]. And Penetration Testing serves as a security provider to test several vulnerabilities present on the Computer and network security [15].

MATERIAL AND METHODS

In this research, the Framework used is Owasp Zap Open Web Application Security Project Zed Attack Proxy (Owasp Zap) with the Pentest Method. OWASP ZAP is a testing tool that can be used as a method to determine if a system has security vulnerabilities [16]. OWASP ZAP offers, develops, and maintains a system for testing security through literature studies, data information searching, and domain information searching[17]. What OWASP ZAP does is to perform attacks on all pages of the website [18]. In penetration testing, the goal is to gather information for review [19]. The process of conducting testing using the Pentest method, where this method is used to evaluate security by simulating attacks on a system, aiming to identify and exploit system vulnerabilities. The methods and framework of OWASP ZAP can be seen in Figure 1.



Source: (Research Results, 2024)
Figure 1. Testing Steps

And for the framework used is the Owasp Zap, where this framework conducts testing on flexible and extensible web applications [20].

he stages carried out using OWASP ZAP are Explore, Attack, and Report, involving scanning to

test servers, networks, and devices using the tools provided by OWASP ZAP. These tools are used as scanners to detect whether there are vulnerabilities in the e-learning system [21].

RESULTS AND DISCUSSION

In an effort to prevent hacking and determine whether the current e-learning system is considered secure, a method is needed to test whether the system has security vulnerabilities that could be exploited by unauthorized parties. Exploitable vulnerabilities include XSS (Cross-Site Scripting) and SQL Injection.

In this pentest method, the steps involved include Pre-Engagement, Intelligence Gathering, and Vulnerability Analysis, Exploitation and Reporting. And the steps in OWASP include Information Gathering, Vulnerability Analysis, and finally, Exploitation.

1. PENTEST

A. Pre-Engagement

The preparation phase as well as the steps of presenting and explaining the tools and techniques that assist in conducting penetration. At this stage, permission to conduct the testing has been obtained from the IBM Bekasi e-learning admin.

B. Intelligence Gathering

At this stage, information gathering regarding pentest testing is conducted. The information successfully collected includes the domain [22]. After obtaining the domain, the next step is to check the e-learning.ibm.ac.id domain using the whois domain tools [23]. The results of the domain information search for e-learning.ibm.ac.id using the pentest method and whois doamin as the tools can be seen in figure 2 below.

Source: (Research Results, 2024)

Figure 2. Result of Whois Domain

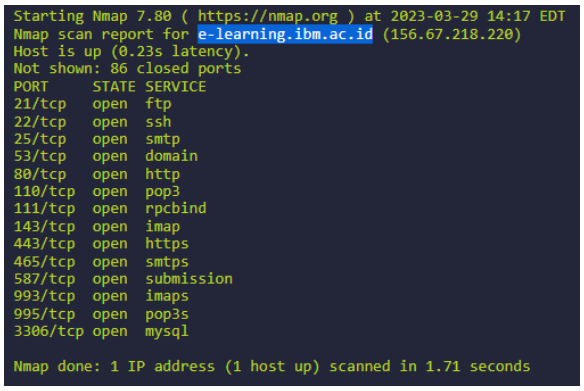
The results of the information search using the pentest method where the tools used is whois domain, if presented in table form, can be clearly seen in table 1 below.

Table 1. Whois Domain Check Results

Domain *e-learning.ibm.ac.id*	
Domain ID	PANDI-DO1241026
Domain Name	ibm.ac.id
Created On	2019-02-18 02:09:02
Last Update On	2024-02-18 04:49:51
Expiration Date	2025-02-18 23:59:59
Status	serverTransferProhibited
Status	clientTransferProhibited
Registrar Organization	PT Registrasi Nama Domain
Registrar Street	Cyber 2 Tower, Lantai 29 JL. HR Rasuna Said X5 No. 13, RT.7/RW.2, Kuningan Kota Jakarta Selatan
Registrar City	Jakarta Selatan
Registrar State/Province	Jakarta Selatan

Source: (Research Results, 2024)

The next step is to conduct network scanning using NMap. This tools is used to discover cybersecurity vulnerabilities of devices by performing scanning. [24]. The results of the scanning using NMap can be seen in Figure 3 below.



Source: (Research Results, 2024)

Figure 3. NMap Scan Results

From the scanning results using the NMap tools in figure 3, if displayed in table form, it shows the ports that can be seen in Table 2 below.

Table 2. NMap Scanning

Domain e-learning.ibm.ac.id		
Port	**State**	**Service**
21/tcp	*Open*	*ftp*
22/tcp	*Open*	*ssh*
25/tcp	*Open*	*Smtp*
53/tcp	*Open*	*domain*
80/tcp	*Open*	*http*
110/tcp	*Open*	*pop3*
111/tcp	*Open*	*rpcbind*
143/tcp	*Open*	*Imap*
443/tcp	*Open*	*https*
465/tcp	*Open*	*smtps*
587/tcp	*Open*	*submission*
993/tcp	*Open*	*imaps*
995/tcp	*Open*	*pop3s*
3306/tcp	*Open*	*mysql*

Source: (Research Results, 2024)

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

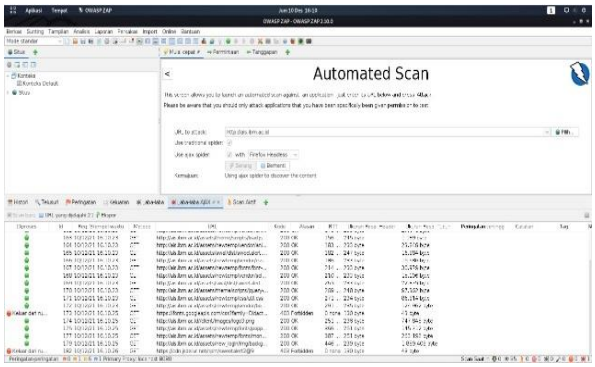
VOL. 10. NO. 2 NOVEMBER 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i2.5534

In the NMap scanning results table 2 above, it shows that all ports on the e-learning domain with IP 172.217.14.206 are recorded as open, making it easier for hackers to exploit weaknesses in the system. Therefore, it can be concluded that the NMap scanning results on the e-learning.ibm.ac.id domain indicate security vulnerabilities that can be exploited by hackers.

After searching for information related to the e-learning.ibm.ac.id domain using the pentest method and the whois domain tools, and NMap, the next stage is to conduct scanning.

C. Vulnerability Analysis

At this stage, identification of e-learning using the domain e-learning.ibm.ac.id is conducted to search for vulnerabilities that could potentially be exploited [25]. Testing is carried out using the Automatic Scan feature, which is part of the Owasp Zap framework. Automatic scanning is performed on the e-learning.ibm.ac.id domain to manually discover vulnerabilities [26]. The scanning process can be seen in Figure 4 below.



Source: (Research Results, 2024)

Figure 4. Automatic Scanning Process

The scanning process in Figure 4 was conducted on the domain e-learning.ibm.ac.id. After the scanning process is completed 100%, the scanning results can be seen in Figure 5 below.

Source: (Research Results, 2024)

Figure 5. OWASP ZAP Scan Results

Based on the scan results using the Owasp Zap tool, 16 vulnerabilities were found. The vulnerabilities that were successfully found can be seen in Table 3.

Table 3. Owasp Zap Scanning Results

No.	Alert Type	Riks
1	Cloud Metadata Potentially Exposed	High
2	Content Security Policy (CSP) Header Not Set	High
3	Missing Anti-clickjacking Header	Medium
4	Tidak adanya token Anti-CSRF	Medium
5	Vulnerable JS Library	Medium
6	Cookie No HttpOnly Flag	Low
7	Cookie without SameSite Attribute	Low
8	Cross-Domain JavaScript Source File Inclusion	Low
9	Private IP Disclosure	Low
10	Strict-Transport-Security Header Not Set	Low
11	X-Content-Type-Options Header Missing	Low
12	Authentication Request Identified	Informational
13	Keterbukaan informasi-komentar mencurigakan	Informational
14	Modern Web Application	Informational
15	Retrieved from Cache	Informational
16	Session Management Response Identified	Informational

Source: (Research Results, 2024)

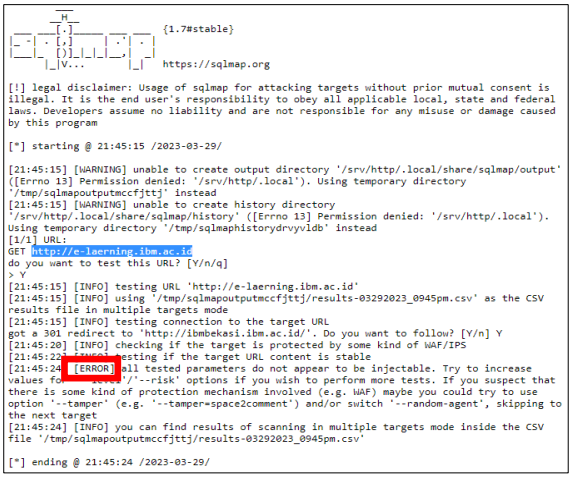
The vulnerability testing using OWASP ZAP shows that there are ten medium-level vulnerabilities, two low-level vulnerabilities, and two high-level vulnerabilities. The two high-level warnings can be described as follows:

1. Cloud Metadata Potentially Exposed" carries a high risk where this attack attempts to misuse misconfigured NGINX servers to access instantly managed metadata by cloud service providers such as AWS, GCP, and Azure.

2. Content Security Policy (CSP) Header Not Set" poses a high risk. Where an additional layer of security that aids in detecting and mitigating certain attacks, including Cross Site Scripting (XSS) and data injection attacks, is not in place. These attacks are utilized for everything from data breaches to destruction and malware dissemination.

D. Exploitation

Exploitation is the next stage, where the focus is on the security used in e-learning.ibm.ac.id [27]. The tools used in this stage are SQLMap. The command executed involves scanning the domain e-learning.ibm.ac.id to determine security information on the system, as shown in Figure 6 below.



Source: (Research Results, 2024)

Figure 6. SQLMap

From the exploitation results in figure 6, by typing the domain e-learning.ibm.ac.id, there was an error indicating that the tested parameter could not be injected.

E. Reporting

Reporting of discovered and exploited vulnerability penetrations [28]. In the final stage of this security vulnerability testing, it can be concluded that the e-learning domain e-learning.ibm.ac.id employs a Vulnerability Analysis approach using OWASP Zap tools and conducts scanning in the exploitation stage using SQLMap tools. From these tests, the report that can be provided on Vulnerabilities includes two vulnerabilities recorded during the scanning phase, while in the exploitation stage, it could not proceed due to an error encountered with the e-learning domain e-learning.ibm.ac.id.

2. Owasp

A. Information Gathering

Similarly to Intelligence Gathering, in this Information Gathering stage, information about the e-learning platform to be tested will be sought using Whois Domain. The information obtained using Whois Domain can be seen in figure 2 and table 1.

B. Vulnerability Analysis

After Information Gathering, the next stage is Vulnerability Analysis. In this stage, scanning is conducted on the e-learning domain to see if there are any vulnerabilities. The tool used is Accunetix vulnerability scanning. The scanning results can be seen in the figure 7 below.

Source: (Research Results, 2024)

Figure 7. Vulnerability Accunetix Result

The results from Accunetix Vulnerability can be explained that on the domain e-learning.ibm.ac.id there are Header Strict-Transport-Security Header Not Set, Missing Anti-clickjacking Header, X-Content-Type-Options Header, and Content Security Policy (CSP) Header Not Set. With these results, there is a potential for exploitation by someone against the e-learning system.

C. Exploitation

In this stage, an attack simulation is conducted on the e-learning platform to search for security loopholes and vulnerabilities using SQL Injection, XSS, and Broken Access Control tools. The results of the attack simulation conducted can be explained in Table 4 below.

Table 4. Result Exploitation

Exploitation	Domain	Result
SQL Injection	http://e-learning.ibm.ac.id/assets/newtemp/vendor/countdowntime/countdown time.js/	Failed
	http://e-learning.ibm.ac.id/assets/newtemp/vendor/bootstrap/js/bootstrap.min.is/	Failed
	http://e-learning.ibm.ac.id/assets/theme/script/load.js?1359456394/	Failed
	http://e-learning.ibm.ac.id/assets/newtemp/js/main.js	Failed
XSS Cross Scripting	http://e-learning.ibm.ac.id/assets/swal#jaVasCript:/	Failed
	http://e-learning.ibm.ac.id/index.php/welcome/login/	Failed
Broken Access Control	http://e-learning.ibm.ac.id/login/index.php/	Failed
	http://e-learning.ibm.ac.id/#c_mahasiswa/view/2366	Failed
	http://e-learning.ibm.ac.id/search/index.php/	Success

Source: (Research Results, 2024)

Based on Table 5 above, it can be concluded that the simulation testing using SQL Injection was unsuccessful, and testing using XSS and Broken Access Control could not be conducted. When the testing was performed on the e-learning domain search, the report indicated success.

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 2 NOVEMBER 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i2.5534

CONCLUSION

This study focuses on testing an e-learning platform using the pentest method with the OWASP ZAP framework. In the previous study, methods and steps included using standard Docker containers to integrate Juice Shop and the ZAP API, as well as running an evolutionary algorithm to calculate scores based on the number of alerts found. Testing on the e-learning platform with the domain e-learning.ibm.ac.id employed pentest methods with several testing stages. For future research, it is necessary to use the latest tools and adopt a broader testing approach. By adopting these future research directions and methodological improvements, the robustness and effectiveness of security testing can be enhanced, providing better protection for critical systems and data.

The first step was Pre-Engagement, involving discussions with e-learning management about the planned testing. The second step was Intelligence Gathering, where information related to the domain e-learning.ibm.ac.id was gathered using Whois Domain tools. The third stage was Vulnerability Analysis, where the domain was scanned using ZAP tools. The scan results using ZAP revealed two high-level vulnerabilities, ten medium-level vulnerabilities, and two low-level vulnerabilities.

The next stage involved exploitation using SQL Map tools, but the SQL Map testing was unsuccessful. Subsequently, testing using OWASP was conducted. The first step in this testing was Information Gathering, which involved searching for domain-related information using Whois Domain tools. The second stage was Vulnerability Analysis, with findings including issues such as Strict-Transport-Security Header Not Set, Missing Anti-clickjacking Header, X-Content-Type-Options Header, and Content Security Policy (CSP) Header Not Set. These issues could potentially allow unauthorized access to the system.

The final stage was Exploitation, where attack simulations were performed on the e-learning platform to identify security vulnerabilities using SQL Injection, XSS, and Broken Access Control tools. The results concluded that the SQL Injection attack simulation was unsuccessful, and testing for XSS and Broken Access Control could not be performed. However, testing on the e-learning domain showed success, which could be a parameter for attackers to obtain information about registered users in the system. For future security research, several steps can be taken to enhance the security of this e-learning platform. Firstly, updating and enhancing security policies, including implementing appropriate security headers such as Strict-Transport-Security, Anti-clickjacking, and Content Security Policy (CSP), is necessary. Additionally, conducting regular and thorough testing using tools like ZAP and SQL Map to identify and mitigate existing vulnerabilities is crucial. Therefore, future security research should focus on strengthening security policies, systematic vulnerability testing, and further developing methodologies to address increasingly complex and evolving security threats.

REFERENCE

[1] P. Vassilakopoulou and E. Hustad, "Bridging Digital Divides: a Literature Review and Research Agenda for Information Systems Research," *Inf. Syst. Front.*, vol. 25, no. 3, pp. 955–969, 2023, doi: 10.1007/s10796-020-10096-3.

[2] C. Collins, D. Dennehy, K. Conboy, and P. Mikalef, "Artificial intelligence in information systems research: A systematic literature review and research agenda," *Int. J. Inf. Manage.*, vol. 60, no. November 2020, p. 102383, 2021, doi: 10.1016/j.ijinfomgt.2021.102383.

[3] R. Sacks, I. Brilakis, E. Pikas, H. S. Xie, and M. Girolami, "Construction with digital twin information systems," *Data-Centric Eng.*, vol. 1, no. 6, p. e14, 2020, doi: 10.1017/dce.2020.16.

[4] M. Bond, K. Buntins, S. Bedenlier, O. Zawacki-Richter, and M. Kerres, "Mapping research in student engagement and educational technology in higher education: a systematic evidence map," *Int. J. Educ. Technol. High. Educ.*, vol. 17, no. 1, pp.1-30, 2020, doi: 10.1186/s41239-019-0176-8.

[5] F. E. Perdima, S. Suwarni, and N. Gazali, "Educational technology in physical education learning: A bibliometric analysis using Scopus database," *Sport TK*, vol. 11, no. 19, pp. 1–16, 2022, doi: 10.6018/sportk.517091.

[6] V. M. Bradley, "Learning Management System (LMS) Use with Online Instruction," *Int. J. Technol. Educ.*, vol. 4, no. 1, p. 68, 2020, doi: 10.46328/ijte.36.

[7] C. Sisavath and L. Yu, "Design and implementation of security system for smart home based on IOT technology," *Procedia Comput. Sci.*, vol. 183, pp. 4–13, 2021, doi: 10.1016/j.procs.2021.02.023.

[8] M. Krishna, S. M. B. Chowdary, P. Nancy, and V. Arulkumar, "A Survey on Multimedia Analytics in Security Systems of Cyber Physical Systems and IoT," *Proc. - 2nd Int.*

Conf. Smart Electron. Commun. ICOSEC 2021, pp. 1–7, 2021, doi: 10.1109/ICOSEC51865.2021.9591754.

[9] C. Chakraborty, S. M. Nagarajan, G. G. Devarajan, T. V Ramana, and R. Mohanty, "Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method," *ACM Trans. Sens. Networks*, 2023, doi: 10.1145/3597210.

[10] A. Y. A. B. Ahmad, S. S. Kumari, S. MahabubBasha, S. K. Guha, A. Gehlot, and B. Pant, "Blockchain Implementation in Financial Sector and Cyber Security System," *2023 Int. Conf. Artif. Intell. Smart Commun. AISC 2023*, pp. 586–590, 2023, doi: 10.1109/AISC56616.2023.10085045.

[11] Nurbojatmiko, A. Lathifah, F. Bil Amri, and A. Rosidah, "Security Vulnerability Analysis of the Sharia Crowdfunding Website Using OWASP-ZAP," *2022 10th Int. Conf. Cyber IT Serv. Manag. CITSM 2022*, pp. 1–5, 2022, doi: 10.1109/CITSM56380.2022.9935837.

[12] S. Alazmi and D. C. De Leon, "A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners," *IEEE Access*, vol. 10, pp. 33200–33219, 2022, doi: 10.1109/ACCESS.2022.3161522.

[13] R. S. Devi and M. M. Kumar, "esting for security weakness of web applications using ethical hacking," n 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 354–361, 2020.

[14] H. S. Abdullah, "Evaluation of Open Source Web Application Vulnerability Scanners," *Acad. J. Nawroz Univ.*, vol. 9, no. 1, p. 47, 2020, doi: 10.25007/ajnu.v9n1a532.

[15] F. Y. Fauzan and Syukhri, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang dari keamanan web adalah sebanyak 96 dengan disimpulkan Acunetix Threat Level 2 yaitu pada level Medium yang artinya tidak," *J. Vocat. Tek. Elektron. dan Inform.*, vol. 9, no. 2, 2021, [Online]. Available: http://ejournal.unp.ac.id/index.php/votekonika/article/download/111778/105248

[16] M. Aydos, Ç. Aldan, E. Coşkun, and A. Soydan, "Security testing of web applications: A systematic mapping of the literature," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6775–6792, 2022, doi: 10.1016/j.jksuci.2021.09.018.

[17] E. R. Flores, "ZAP Proxy and OWASP Top 10". *Computer Science,* 2023

[18] E. Serrano-Collado, M. Garcia-Valdez, and J. J. Merelo-Guervos, "Improving evolution of service configurations for moving target defense," *2020 IEEE Congr. Evol. Comput. CEC 2020 - Conf. Proc.*, pp. 1-8, 2020, doi: 10.1109/CEC48606.2020.9185786.

[19] E. A. Altulaihan, A. Alismail, and M. Frikha, "A Survey on Web Application Penetration Testing," *Electron.*, vol. 12, no. 5, p. 1229, 2023, doi: 10.3390/electronics12051229.

[20] Jobin T.J and Karthika Suresh Babu, "26Owasp_Zed_Attack_Proxy," *Natl. Conf. Emerg. Comput. Appl.*, vol. 3, no. 1, pp. 106–111, 2021.

[21] M. Gibran, A. Danialdo, F. A. Bakhtiar, and M. Data, "Pengujian Efektivitas OWASP ZAP dalam Menemukan Kerentanan dari Metasploitable," vol. 7, no. 7, pp. 3431–3433, 2023.

[22] D. N. Astrida, A. R. Saputra, and A. I. Assaufi, "Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES)," *Sinkron*, vol. 7, no. 1, pp. 147–154, 2022, doi: 10.33395/sinkron.v7i1.11249.

[23] Z. A. Khan, "Penetration Testing Information System Security Assessment Framework (ISSAF)," *Penetration Testing Information System Security Assessment Framework (ISSAF),* vol. 4 no. 3, pp. 1593-1601, 2023.

[24] I. Nedyalkov, "Study the Level of Network Security and Penetration Tests on Power Electronic Device", Computers, vol. 13, no. 3, p. 81, 2024.

[25] P. Zeng, G. Lin, L. Pan, Y. Tai, and J. Zhang, "Software vulnerability analysis and discovery using deep learning techniques: A survey," *IEEE Access*, vol. 8, pp. 197158–197172, 2020, doi: 10.1109/ACCESS.2020.3034766.

[26] Q. Zhang and F. Li, "Cyber-Vulnerability Analysis for Real-Time Power Market Operation," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3527–3537, 2021, doi: 10.1109/TSG.2021.3066398.

[27] F. Heiding, E. Süren, J. Olegård, and R. Lagerström, "Penetration testing of connected households," *Comput. Secur.*, vol. 126, 2023, doi: 10.1016/j.cose.2022.103067.

[28] F. L. Færøy, M. M. Yamin, A. Shukla, and B. Katt, "Automatic Verification and Execution of Cyber Attack on IoT Devices," *Sensors*, vol. 23, no. 2, pp. 1–30, 2023, doi: 10.3390/s23020733.