

Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap

Fauzan Prasetyo Eka Putra^{1*}, Ubaidi², Amir Hamzah³, Walid Agel Pramadi⁴, Alief Nuraini⁵

^{1,2,3,4}Program Studi Informatika Fakultas Teknik Universitas Madura, Jl. Raya Panglegur KM 3,5 Pamekasan 69371 Indonesia

¹prasetyo@unira.ac.id, ²ubed@gmail.com, ³amirzha03@gmail.com, ⁴walidagel99@gmail.com,

⁵aliefnuraini3@gmail.com



ABSTRACT

*Corresponding Author

Article History:

Submitted: 04-07-2024

Accepted: 04-07-2024

Published: 22-07-2024

Keywords:

OWASP, Vulnerability Detection, Web Security, SQL Injection, Security Testing

Brilliance: Research of Artificial Intelligence is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

This research highlights the detection of security vulnerabilities on websites using OWASP ZAP, a highly regarded open-source web security testing tool. Through a comprehensive literature review approach and systematic research methodology, this research emphasizes the urgency of addressing the ever-evolving security threats in web systems. Web security is a crucial aspect of information technology as more and more sensitive data is transmitted through web applications. OWASP ZAP, recognized for its reliability in identifying various security holes, was used to evaluate its effectiveness and efficiency in detecting vulnerabilities in web applications. This tool assists developers and security researchers in finding and fixing weaknesses that could be exploited by attackers. The results of the study show that OWASP ZAP is not only effective in identifying vulnerabilities such as SQL Injection, XSS (Cross-Site Scripting), and misconfiguration but also provides practical solutions to strengthen overall web security. Additionally, this research identifies several challenges faced when using OWASP ZAP and offers recommendations to address these issues. This study makes a significant contribution towards a better understanding of web security and offers recommendations for the implementation of better security testing tools in web development environments. Consequently, this research encourages the adoption of more proactive and systematic security practices in web application development.

INTRODUCTION

With the advancement of information technology that continues to develop from year to year, the need to secure data is becoming increasingly urgent (Prasetyo Eka Putra, 2023) (Putra et al., 2024). Along with the rapid advancement of technology, data security is an issue that needs to be addressed immediately (Zulfikri et al., 2023) (Haidar Hari, Eka Putra, Hasanah, Sutarsih, & Riyan, 2023). The number of cyberattacks on the internet has significantly increased in recent years, resulting in financial and reputational losses for many organizations (Eka Putra, Amir Hamzah, Agel, & Firmansyah Kusuma, 2024). Therefore, it is important to pay attention to the security of information systems from threats originating from internal and external sources, both from within the system and from outside the system, because this can cause instability in the system (Pendidikan & Konseling, 2022). To guarantee data integrity and availability, proper preventive measures are required, such as the implementation of strong security protocols and continuous monitoring. Raising employee awareness and training on cybersecurity practices is also an important component in keeping data safe. In situations like this, security testing technologies such as OWASP ZAP can be very helpful in finding and fixing security issues before they are used by irresponsible parties.

SQL injection is one of the security holes in web applications that allows attackers to modify or insert SQL commands into the exchange between the client and the database server (Baklizi et al., 2022) (Alghawazi, Alghazzawi, & Alarifi, 2022). With this loophole, an attacker can steal, damage, or gain unauthorized access to the database. Sensitive data and information stored in these web application databases are vulnerable to security risks (Abdullayev & Chauhan, 2023). Therefore, it is important to prevent attacks on websites in the first place in order to improve system security and prevent data leakage (Fariadi & Redo Islami, 2022). The use of strict input validation, the use of parameterized queries, and the implementation of strong authentication mechanisms can help reduce the possibility of SQL injection attacks. Additionally, using automated security testing tools such as OWASP ZAP can help find possible vulnerabilities before an attack occurs. An effective cybersecurity strategy also requires increased surveillance and regular security evaluations to protect systems from new threats that are constantly emerging.

OWASP ZAP, developed by the OWASP organization, is one of the most popular and well-maintained open source web security testing tools (Mansur, 2023) (Jakobsson & Haggström, 2022). It is often used by beginners in understanding application security and also by very active penetration testing professionals, and has been recognized as an excellent tool (Kalaani, 2023) (I. F. A. Ashari, Affandi, Putra, & Nur, 2023). OWASP ZAP offers various features that



allow users to perform automated scans of security vulnerabilities in web applications as well as providing detailed reports that help in understanding and fixing such gaps. OWASP ZAP is an ideal tool for people with varying levels of expertise, ranging from individual developers to large enterprise security teams. In addition, OWASP's active community of users and developers ensures that OWASP ZAP is constantly updated with the latest security features and fixes, keeping the tool relevant in the face of ever-evolving cyber threats. OWASP ZAP helps organizations adopt a proactive approach to finding and addressing vulnerabilities, improving overall web application security. Integrating OWASP ZAP into the web application development lifecycle also helps ensure that security practices are followed from the beginning to the final stages of development, resulting in a more secure environment for end users.

Previous researchers, such as (Taryana & Heryana, 2023)(Ilmi, Seta, & Pradnyana, 2022)(Wibowo, Ardi Susanto, & Khibar Pusaka, 2022) have conducted research on security holes on websites using various different frameworks. The application of frameworks aims to set standards in conducting effective system security testing (Burhani & Priyawati, 2024). This article will discuss the concept and application of security gap detection on websites using OWASP ZAP, using the Literature Review method (Azahra, 2023). By providing clear and in-depth guidelines on how to use OWASP ZAP as a tool to detect vulnerabilities in web applications, this research is expected to make a significant contribution to the field of cybersecurity. Various previous studies and research findings will be analyzed through the literature review method. The purpose of this is to find trends, problems, and solutions that have been found in web application security testing. OWASP ZAP was chosen because it is very flexible and can be integrated with various development tools and platforms. The tool is also known for its ability to perform complex scans and generate thorough reports; this is very beneficial to developers and security teams in fixing their system weaknesses. This research is expected to help organizations adopt the best security testing methods and increase organizational awareness of the importance of implementing ZAP.

LITERATURE REVIEW

Literature studies are generally used to refer to the process of compiling and evaluating various literature sources related to a research topic or research (S. F. Arief & Sugiarti, 2022). Conducting literature reviews from books and journals that focus on related theories, especially in the domain of security management and information system security (Fadla Silvia, Saputra, Sunaryo, & Sinlae, 2024). The sources for the systematic study of literature were obtained through an online search of international journals via Google Scholar (Mutedi & Tjahjono, 2022).

It is important to consider the quality and relevance of each source accessed when conducting the literature review. Evaluating the methodologies, findings and results of previous studies helps to ensure that the theoretical foundations used are strong and reliable. Additionally, compiling a comprehensive literature allows researchers to discover unfilled research gaps and room for additional research. This process not only adds to one's knowledge, but also provides a more in-depth view of how the theories can be applied in the real world. Therefore, an accurate literature review provides a solid foundation for further research.

METHOD

Research methodology is a series of steps, processes, flows, rules, and procedures that will be used by a researcher (Aldisa & Wahyuddin, 2022). The following is a research method that shows the stages in the research process (Mulyanto, Zaen, Yuliadi, & Sihab, 2022).

Problem Identification

In this first stage is to identify insecure websites (Willy Andrian & Dedy Prasetya Kristiadi, 2022). The more vulnerabilities that exist in a website application, the more vulnerable the website is to attacks that can cause piracy or hacking of data (I. F. Ashari, Rizta Anugrah P, Andintya W, & Denira, 2023)(Al'am'yubi & Wijayanto, 2023). A critical first step to maintaining the security and integrity of a website is finding these vulnerabilities.

In this process, various security elements are thoroughly examined. This includes testing for possible loopholes that can be exploited by attackers. These errors can stem from poor source code, incorrect configuration, or even the use of aging software. Additionally, the identification process often utilizes automated tools that have the ability to scan websites for potential threats. Once vulnerabilities are discovered, the next step is to evaluate how each gap could impact the system as a whole.

Therefore, vulnerabilities that have the most impact can be given priority. In addition, problem identification should be an iterative process. The cyber world is constantly evolving, and the threats that come with it as well. Therefore, constant monitoring and updating of security systems is essential. Employee training and awareness of cybersecurity best practices is also an important part of the approach to identifying and mitigating these risks. Comprehensive and sustainable methods allow organizations to be more proactive in protecting their digital assets from the ever-evolving range of cyber threats.

Study Selection

There were a total of 55 literature titles found during the search using the initial keywords and with a publication year range of 2022-2024 (Eka Putra et al., 2024). Study selection was done accordingly by selecting some relevant articles (Studi, Informatika, Teknik, & Nusantara, 2024). After the initial discovery, a more in-depth review of the abstracts and content of the articles was conducted to assess suitability to the research topic. Only journals were selected as research sources, as they are considered more accurate and up-to-date in presenting research findings than books which may not cover the latest developments in the field (M. F. Arief, Santoso, & Kurniawan, 2022). The use of appropriate keywords and specific timeframes helped to filter out literature that met our research criteria. This selection was done by considering the quality and credibility of the journals, as well as their potential impact and contribution to the current research. Thus, study selection is an important step in ensuring that the analysis and findings are based on the most relevant and reliable literature.

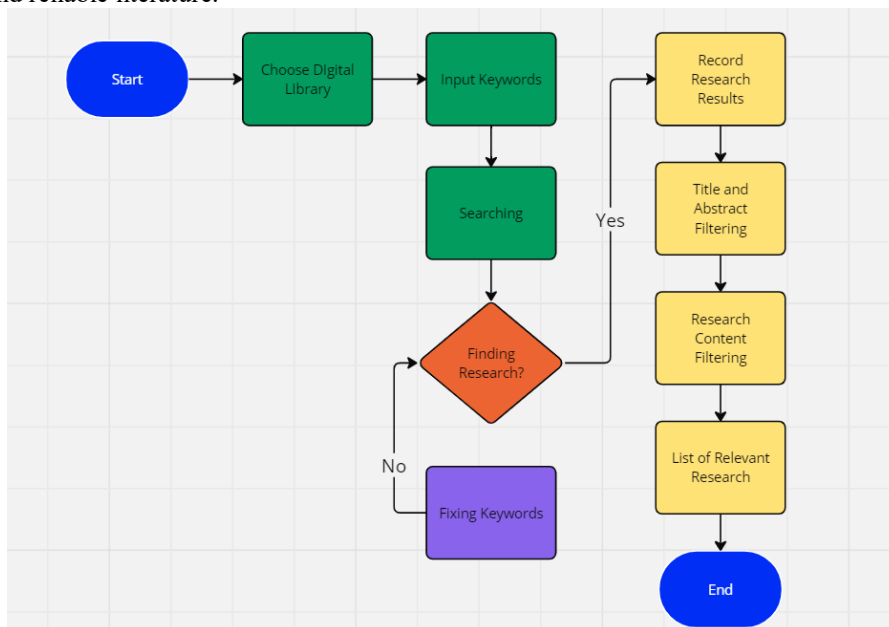


Figure 1. Flowchart Study Selection

RESULT

Nowadays web application vulnerabilities for example SQL Injection are becoming more common and more frequently reported (Alazmi & De Leon, 2022). If web applications are built without following the latest security guidelines and practices, they may be vulnerable to cyberattacks (Abdulghaffar, Elmrahit, & Yousefi, 2023). Therefore, a vulnerability scanner application was created to help find vulnerabilities in web-based applications and networks (Kurniawan & Ramli, 2023).

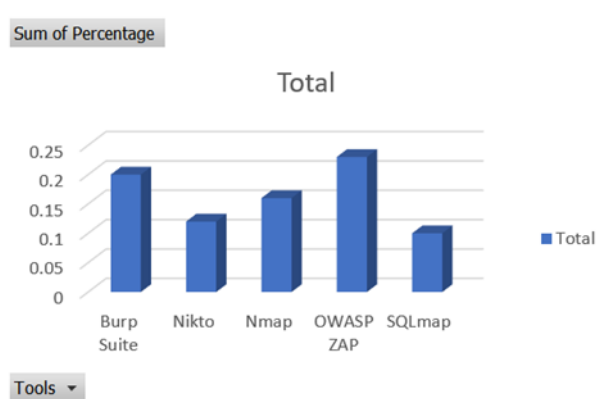


Figure 2. Web security gap detection tools

Based on the Open WEB Application Security Project (OWASP) report, SQL injection attacks are recognized as one of the most dangerous threats to web applications and ranked third among threats in 2022 (Hasan, Al-Maliki, & Jasim, 2022) (Pratama, Songida, & Gunawan, 2022). This penetration test, using the OWASP framework, successfully

identified several security vulnerabilities on the target website (Kristara & Adiguna, 2023). The various vulnerability testing methods presented above are grouped by year of discovery in Figure 3 (Dewi, 2022).

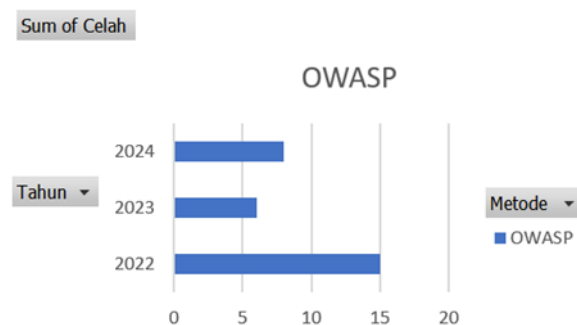


Figure 3. Test results based on year

From the previous classification analysis, it can be concluded that the OWASP method is more commonly used in security vulnerability testing (Sembiring, Sidiq, & Prabowo, 2024). From the results of security testing using OWASP Zap, several vulnerabilities were found on the website. Information related to these vulnerabilities can be found in the summary sentence that presents the OWASP Top 10 (Mu'min, Fadlil, & Riadi, 2022)(Riandhanu, 2022).

There is a time difference between the two vulnerability scanners although the results have certain similarities. This difference occurs due to the smaller number of scanning requests from the kabupaten government compared to the village government, so the process can be completed more quickly. In addition, there were variations in the types of vulnerabilities found. On the semarangkab.go.id web, vulnerabilities at the medium threat level were identified using the OWASP Top 10, indexed in A06: 2017 Security Misconfiguration, A3: 2017-Sensitive Data Exposure, and A09: 2017 Using Components with Known Vulnerabilities in Pentest-Tools. As for the low threat level, both OWASP documents are parameters for both web vulnerability scanning tools (Darojat, Sediyo, & Sembiring, 2022).

DISCUSSION

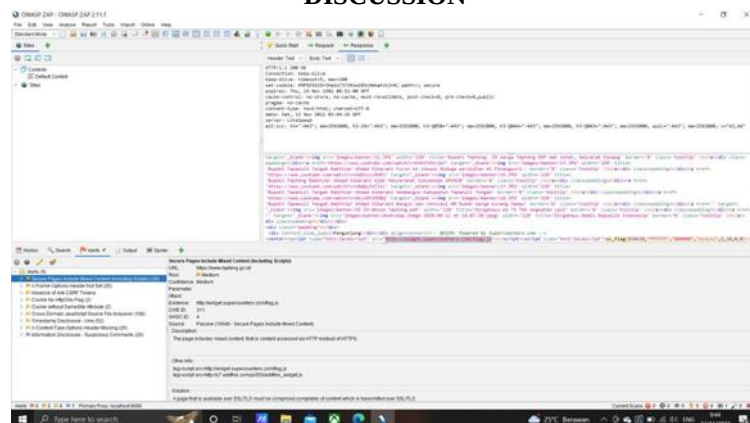


Figure 4. Scanning results of Tapanuli Web using OWASP ZAP

Based on the research results in Figure 4 above conducted by (Nisa, Putra, Siregar, & Dedi Irawan, 2022), In this study, the Zed Attack Proxy (ZAP) method from the Open Web Application Security Project (OWASP) was used to check the security of the Central Tapanuli website (192.187.99.170). The main goal was to find possible security problems and provide advice on how to strengthen the security of the website. According to the OWASP methodology, security testing is carried out through several stages, such as information collection, session management testing, data validation testing, and web service testing.

The scanning results using OWASP ZAP show several levels of threats detected. No High level threats were found, but 4 medium level threats, 7 low level threats, and 1 Informational level threat were detected. The most detected threat was Timestamp Disclosure - Unix with 22,079 instances, despite being at the Low level. This shows that the website has many exploitable timestamps, but the risk is relatively low.

The medium level threats detected include Application Error Disclosure, Secure Pages Include Mixed Content, Vulnerable JS Library, and X-Frame-Options Header Not Set. These threats indicate the potential for information leakage, security issues related to mixed content, use of vulnerable JavaScript libraries, and potential clickjacking

attacks.

For each detected threat, this research provides solutions to mitigate the security risks. Some of the suggested solutions include implementing custom error pages, ensuring all content is accessed via SSL/TLS, upgrading jQuery and other JavaScript libraries, implementing HTTP X-Frame-Options headers, using anti-CSRF tokens, implementing HttpOnly flags on cookies, ensuring JavaScript file sources come from trusted sources, implementing proper cache-control headers, and removing comments containing sensitive information from source code.

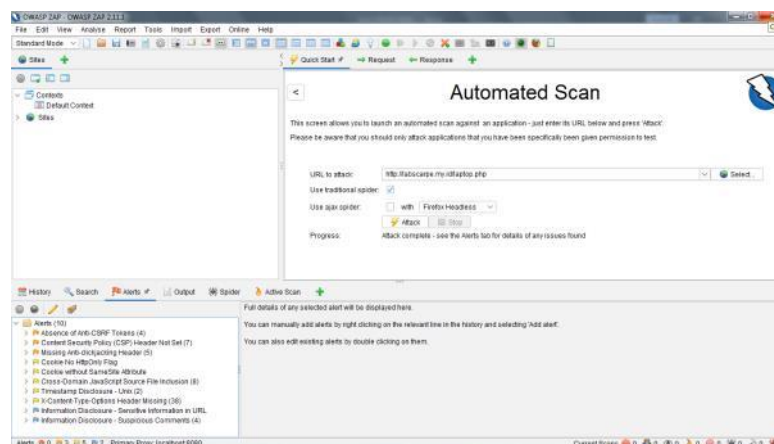


Figure 5. LabScarpe Website Scanning Results

In research conducted by (Hasibuan & Handoko, 2023) based on Figure 5 above, the implementation of OWASP ZAP is carried out to identify vulnerabilities or gaps on the labscarpe.my.id website; the results show eight vulnerabilities that have been identified, including three medium level vulnerabilities and five low level vulnerabilities. There are three medium-level vulnerabilities identified, namely no Anti-CSRF Tokens, no Anti-clickjacking Header, and no Anti-clickjacking Header. On the other hand, five low-level vulnerabilities were identified: Cookie No HttpOnly Flag, Cookie without SameSite attribute, Cross-Domain Source JavaScript File Merge, Missing Timestamp-Type-Option Header, and X-Content-Type-Option Header.

Due to the lack of a protection mechanism against Cross-Site Request Forgery (CSRF) attacks, the Lab.Scarpe website is vulnerable to such attacks. The lack of Anti-CSRF Token demonstrates this. In addition, the Not Set Content Security Policy (CSP) Header vulnerability indicates that the website does not have sufficient content security policies, which increases the risk of Cross-Site Scripting (XSS) attacks. Furthermore, the Missing Anti-clickjacking Header vulnerability indicates that the website is not properly protected from clickjacking attacks.

On the other hand, the five low-level vulnerabilities also provide important information related to the security of the Lab.Scarpe website. For example, the Cookie No HttpOnly Flag vulnerability indicates that the cookie used does not have the HttpOnly flag, which may increase the risk of user information theft. The Cookie without SameSite Attribute vulnerability indicates that the cookie does not have the SameSite attribute, which can be exploited for CSRF attacks. In addition, the Cross-Domain JavaScript Source File Inclusion vulnerability reveals a loophole that allows attackers to insert JavaScript files from other domains into a website, increasing the risk of XSS attacks.

Furthermore, the Timestamp-Type-Option Header Missing vulnerability indicates that the Timestamp-Type-Option header is not set correctly, which may affect the security of the website against certain attacks. Finally, the X-Content-Type-Option Header vulnerability indicates that the X-Content-Type-Option header is not optimally set, increasing the risk of MIME sniffing attacks.

By identifying and evaluating these vulnerabilities, the implementation using OWASP ZAP on the Lab.Scarpe website provides valuable insight into the security level of the website. Security measures can be taken based on the results of this evaluation to increase the website's resilience against various cyber-attacks. Through this implementation, the website owner can fix existing vulnerabilities and improve the protection of user data and the overall integrity of the website.

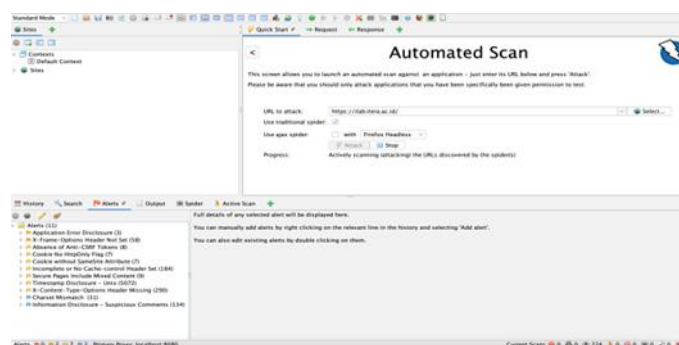


Figure 6. Scanning Results of the Itera Lab Website

The security audit results shown in Figure 6 (I. F. A. Ashari et al., 2023) show that there are high, medium, low, and information level vulnerabilities on the ilab.itera.ac.id website. High-level vulnerabilities include one SQL injection security vulnerability, while medium-level vulnerabilities include application error disclosure vulnerabilities, vulnerable js libraries, unregulated x-frame-options headers. Meanwhile, low-level vulnerabilities include the absence of anti CSRF tokens, cookies without HttpOnly attributes, cookies without equal attributes, and cross-domain JavaScript scripts.

In the study, vulnerability testing steps (security audit) were carried out using the OWASP ZAP tool. The audit results show that the ilab.itera.ac.id website has insecure vulnerabilities, so it needs to be repaired to strengthen protection to keep it protected from those who intend to harm the website. Recommendations from this security audit include to regularly check and improve website security.

This research also emphasizes the importance of vulnerability testing to identify and address vulnerability risks that may be faced by an information system. By conducting a security audit, it can be seen what vulnerabilities exist on the website and what steps need to be taken to fix them. The vulnerability testing method using OWASP ZAP has proven effective in detecting security vulnerabilities on websites, such as those carried out on the ITERA UPT Terpadu Laboratorium (Ilab) website.

CONCLUSION

This research successfully reveals the importance of security vulnerability detection on websites by using OWASP ZAP, a reliable and effective open-source web security testing tool. Through in-depth analysis and application of a comprehensive methodology, this research shows that OWASP ZAP is able to effectively identify various types of security vulnerabilities, including SQL Injection, misconfiguration, and exposure of sensitive data. The results of this study confirm that the implementation of OWASP ZAP not only significantly improves the security of web applications, but also provides a systematic framework for vulnerability detection and mitigation.

This study provides valuable insights for cybersecurity practitioners and web developers, by emphasizing the need for the integration of security testing tools such as OWASP ZAP in the web application development process. By adopting a proactive approach in identifying and fixing security gaps, organizations can reduce the risk of cyberattacks and protect the integrity and confidentiality of their data. The research also suggests that training and education on the use of web security testing tools should be increased to ensure that all parties involved in web application development and maintenance have a deep understanding of security best practices.

Overall, this research confirms that OWASP ZAP is a highly effective tool for the detection and mitigation of security vulnerabilities in web applications, and is an essential component in a comprehensive web security strategy. Going forward, further research can be conducted to explore the integration of OWASP ZAP with other security tools and technologies to enhance protection against increasingly complex cyber threats.

REFERENCES

- Abdulghaffar, K., Elmrabit, N., & Yousefi, M. (2023). Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners. *Computers*, 12(11), 1–17. <https://doi.org/10.3390/computers12110235>
- Abdullayev, V., & Chauhan, A. S. (2023). SQL Injection Attack: Quick View. *Mesopotamian Journal of CyberSecurity*, 2023, 30–34. <https://doi.org/10.58496/MJCS/2023/006>
- Al'am'yubi, M. R. S. ., & Wijayanto, D. . (2023). Analisis Sistem Keamanan Website XYZ Menggunakan Framework OWASP ZAP. *Jurnal Ilmu Komputer (JUIK)*, 3(1), 1–5. Retrieved from <https://journal.umgo.ac.id/index.php/juik/index>
- Alazmi, S., & De Leon, D. C. (2022). A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners. *IEEE Access*, 10, 33200–33219. <https://doi.org/10.1109/ACCESS.2022.3161522>

- Aldisa, R. T., & Wahyuddin, M. I. (2022). Sistem Informasi Laboratorium Dengan Metode Joint Application Design (JAD) Berbasis Website (Kasus: Laboratorium Artificial Intelligence Universitas Nasional). *Jurnal Sains Komputer & Informatika (J-SAKTI)*, 6(1), 553.
- Alghawazi, M., Alghazzawi, D., & Alarifi, S. (2022). Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*, 2(4), 764–777. <https://doi.org/10.3390/jcp2040039>
- Arief, M. F., Santoso, N. A., & Kurniawan, R. D. (2022). Systematic Literatur Review: Keamanan Komputer Pada Jaringan Nirkabel. *Indonesia Journal of Internasional Relations (IJIR)*, 3(2), 1–8.
- Arief, S. F., & Sugiarti, Y. (2022). Literature Review: Analisis Metode Perancangan Sistem Informasi Akademik Berbasis Web. *Jurnal Ilmiah Ilmu Komputer*, 8(2), 87–93. <https://doi.org/10.35329/jiik.v8i2.229>
- Ashari, I. F. A., Affandi, M., Putra, H. T., & Nur, M. T. (2023). Security Audit for Vulnerability Detection and Mitigation of UPT Integrated Laboratory (ILab) ITERA Website Based on OWASP Zed Attack Proxy (ZAP). *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, 7(1), 24–34. <https://doi.org/10.35870/jtik.v7i1.657>
- Ashari, I. F., Rizta Anugrah P, L., Andintya W, N., & Denira, S. T. (2023). Analisis Celah Keamanan Dan Mitigasi Website E-Learning Itera Menggunakan Owasp Zed Attack Proxy (Zap) Vulnerability and Mitigation Analysis of the Itera E-Learning Website Using Owasp Zed Attack Proxy (Zap). *Dinamika Rekayasa*, 19(1), 29–35.
- Azahra, Z. (2023). *Systematic Literature Review (SLR) : Sistem Informasi Donor Darah Berbasis Teknologi*. 7, 31236–31242.
- Baklizi, M., Atoum, I., Abdullah, N., Al-Wesabi, O. A., Ootom, A. A., & Hasan, M. A. S. (2022). A Technical Review of SQL Injection Tools and Methods: A Case Study of SQL Map. *International Journal of Intelligent Systems and Applications in Engineering*, 10(3), 75–85.
- Burhani, L. F., & Priyawati, D. (2024). Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (Ptes). *JUPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, 9(1), 307–319. Retrieved from <https://jurnal.stkipggritlungagung.ac.id/index.php/jupi/article/view/4455>
- Darojat, E. Z., Sediyo, E., & Sembiring, I. (2022). Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner. *Jurnal Sistem Informasi Bisnis*, 12(1), 36–44. <https://doi.org/10.21456/vol12iss1pp36-44>
- Dewi, B. T. K. & M. A. S. (2022). Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web. *Automata*, 3(1), 1–8. Retrieved from <https://journal.uui.ac.id/AUTOMATA/article/view/21883/12030>
- Eka Putra, F. P., Amir Hamzah, Agel, W., & Firmansyah Kusuma, R. O. (2024). Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking. *Jurnal Sistim Informasi Dan Teknologi*, 5(4), 82–87. <https://doi.org/10.60083/jsisfotek.v5i4.329>
- Fadla Silvia, A., Saputra, W., Sunaryo, H., & Sinlae, F. (2024). Analisis Keamanan Data Pribadi pada Pengguna BPJS Kesehatan: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Nusantara Journal of Multidisciplinary Science*, 2(1), 201–207. Retrieved from <https://jurnal.intekom.id/index.php/njms>
- Fariadi, F., & Redo Islami, M. R. (2022). Deteksi Dini Serangan Pada Website Menggunakan Metode Anomali Based. *JIKO (Jurnal Informatika Dan Komputer)*, 5(3), 224–229. <https://doi.org/10.33387/jiko.v5i3.5352>
- Haidar Hari, N., Eka Putra, F. P., Hasanah, U., Sutarsih, S. R., & Riyan. (2023). Transformasi Jaringan Telekomunikasi dengan Teknologi 5G: Tantangan, Potensi, dan Implikasi. *Jurnal Informasi Dan Teknologi*, 5(2), 146–150. <https://doi.org/10.37034/jidt.v5i2.357>
- Hasan, M., Al-Maliki, A., & Jasim, N. (2022). Review of SQL injection attacks: Detection, to enhance the security of the website from client-side attacks. *Int. J. Nonlinear Anal. Appl*, 13(October 2021), 2008–6822. Retrieved from <http://dx.doi.org/10.22075/ijnaa.2022.6152>
- Hasibuan, A. F., & Handoko, D. (2023). Analisis Keretakan Website Dengan Aplikasi Owasp Zap. *Jurnal Ilmu Komputer Dan Sistem Informasi*, 2(2), 257–270. Retrieved from <https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/51>
- 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. *Informatik : Jurnal Ilmu Komputer*, 18(2), 190. <https://doi.org/10.52958/iftk.v18i2.4672>
- Jakobsson, A., & Häggström, I. (2022). *Study of the techniques used by OWASP ZAP for analysis of vulnerabilities in web applications*. 61. Retrieved from <https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1675227&dsid=-4307>
- Kalaani, C. (2023). *OWASP ZAP vs snort for SQLi vulnerability scanning*. Retrieved from <https://digitalcommons.georgiasouthern.edu/etd>
- Kristara, F. S., & Adiguna, M. A. (2023). Pengujian Celah Keamanan Input Validation Pada Aplikasi Website Menggunakan Framework Owasp. *Jurnal Penelitian Ilmu Komputer*, 1(4), 50–55.
- Kurniawan, A., & Ramli, K. (2023). Effectiveness of Security Through Obscurity Methods To Avoid Web Application Vulnerability Scanners. *Jurnal Teknik Informatika (Jutif)*, 4(6), 1479–1486.

- <https://doi.org/10.52436/1.jutif.2023.4.6.778>
- Mansur, N. H. (2023). *Vulnerability analysis using OWASP ZAP on higher education websites*. 2665(1). <https://doi.org/10.1063/5.0153145>
- Mu'min, M. A., Fadlil, A., & Riadi, I. (2022). Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework. *Jurnal Media Informatika Budidarma*, 6(3), 1468. <https://doi.org/10.30865/mib.v6i3.4099>
- Mulyanto, Y., Zaen, M. T. A., Yuliadi, Y., & Sihab, S. (2022). Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest). *Journal of Information System Research (JOSH)*, 4(1), 202–209. <https://doi.org/10.47065/josh.v4i1.2335>
- Mutedi, A., & Tjahjono, B. (2022). Systematic Literature Review: Preventing SQL Injection Attacks Using Tools OWASP CSR Web Application Firewall. *Maret*, 7(1), 151–156. Retrieved from <http://openjournal.unpam.ac.id/index.php/informatika>
- Nisa, K., Putra, M. A., Siregar, R. A., & Dedi Irawan, M. (2022). Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap). *Bulletin of Information Technology (BIT)*, 3(4), 308–216. <https://doi.org/10.47065/bit.v3i4.389>
- Pendidikan, J., & Konseling, D. (2022). Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment. *Jurnal Pendidikan Dan Konseling*, 4(4), 6298–6309.
- Prasetyo Eka Putra, F. (2023). Sleep Mode: Strategi Efisiensi Wireless Sensor Network. *Informatics for Educators And Professionals : Journal of Informatics*, 8(1), 52–56.
- Pratama, T. I. M., Songida, M. D. F., & Gunawan, I. (2022). Analisis Serangan dan Keamanan pada SQL Injection: Sebuah Review Sistematis. *JIIFKOM (Jurnal Ilmiah Informatika Dan Komputer)*, 1(2), 27–32. <https://doi.org/10.51901/jiifkom.v1i2.230>
- Putra, F. P. E., Fauzan, F., Syirofi, S., Mursidi, M., Wahid, D., & Nuraini, A. (2024). Sistem Pengendali Lingkungan Pertanian Dengan Wireless Sensor Network Untuk Mengoptimalkan Budidaya Hidroponik. *Digital Transformation Technology*, 3(2), 931–937. <https://doi.org/10.47709/digitech.v3i2.3461>
- Riandhanu, I. O. (2022). Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi. *Jurnal Informasi Dan Teknologi*, 4(3), 160–165. <https://doi.org/10.37034/jidt.v4i3.236>
- Sembiring, B. P., Sidiq, M. F., & Prabowo, W. A. (2024). *Analisis Keamanan Sistem Informasi Menggunakan Metode Open Web Application Security Project (Owasp)*. 8(3), 3049–3054.
- Studi, P., Informatika, T., Teknik, F., & Nusantara, U. D. (2024). *SYSTEMATIC LITERATURE REVIEW : SERANGAN DEFACE*. 14(2), 106–112.
- Taryana, Y., & Heryana, N. (2023). Analisis Keamanan Website Bpjs Kesehatan Menggunakan Metode Vulnerability Asesement. *Joutica*, 8(1), 31–37. <https://doi.org/10.30736/informatika.v8i1.951>
- Wibowo, D. S., Ardi Susanto, & Khibar Pusaka. (2022). Analisis dan Pengujian Celah Keamanan pada Website DIV Teknik Informatika Politeknik Harapan Bersama. *JURNAL PILAR TEKNOLOGI Jurnal Ilmiah Ilmu Ilmu Teknik*, 7(1), 1–10. <https://doi.org/10.33319/piltek.v7i1.114>
- Willy Andrian, & Dedy Prasetya Kristiadi. (2022). Pengembangan Manajemen Keamanan Informasi Database Dan Aplikasi Dengan Optimasi Keamanan Website. *Jurnal Sistem Informasi Dan Teknologi (SINTEK)*, 2(2), 63–68. <https://doi.org/10.56995/sintek.v2i2.48>
- Zulfikri, A., Putra, F. P. E., Huda, M. A., Hasbullah, H., Mahendra, M., & Surur, M. (2023). Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking. *Digital Transformation Technology*, 3(2), 857–863. <https://doi.org/10.47709/digitech.v3i2.3379>