SECURITY ANALYSIS OF COLLEGE WEBSITES USING VULNERABILITY ASSESSMENT METHOD

Dio Wahyu Saputra[1], Risqy Siwi Pradini [2], Mochammad Anshori [3]
[1,2,3] Informatika, Fakultas Teknologi dan Sains, Institut Teknologi, Sains, dan Kesehatan RS dr. Soepraoen Kesdam V/BRW, Jl. S. Supriadi No.22 Sukun, Malang, Indonesia.
risqypradini@itsk-soepraoen.ac.id

ABSTRACT

Web application security, especially on college websites, is a critical aspect in maintaining data integrity and protecting users from cyber threats. This research evaluates the security of college websites using the vulnerability assessment method. By utilizing tools such as OWASP ZAP and penetration testing techniques, this research identifies weaknesses at various security layers, including vulnerabilities to Path Traversal attacks, SQL Injection, and deficiencies in the implementation of HTTP security header settings. The research shows that a lack of input validation, inadequate security configuration, and the use of outdated software libraries causes the main vulnerabilities. This research proposes some practical solutions such as strengthening security configurations, system updates, and implementing modern security policies to mitigate risks. These findings aim to enhance the security of college websites and create a safer online environment.

Keyword : *website security, security analysis, vulnerability assesment*

1. INTRODUCTION

The digitalization era has brought about a fundamental transformation in the management of higher education institutions, especially in implementing website-based systems for academic and administrative services [1][2]. Today's higher education information systems manage sensitive data, such as student personal information, educational data, financial transactions, and research documentation, which require high security [3][4]. Vulnerabilities in the security systems of higher education institutions' websites have become a serious concern as the complexity and frequency of cyber-attacks increases, which can result in data leaks and service disruptions [5][6].

Research shows that many higher education institutions have not implemented security mechanisms capable of protecting their digital infrastructure, especially in the face of evolving cyber threats [2][7]. These vulnerabilities cover a wide range of aspects, from technical vulnerabilities in application code to insecure server configurations, to deficiencies in comprehensive security policies [8][9]. Recent studies reveal that online academic systems frequently deal with serious threats such as SQL injection, cross-site scripting, remote code execution, and various other forms of vulnerability that can compromise the integrity of the system [10][11][12].

Vulnerability Assessment has proven to be an effective approach to identify vulnerabilities in website security systems, with the ability to detect varying levels of security risks [13][5]. This methodology allows for a comprehensive analysis of various security aspects, including network infrastructure, access management, data protection, and web application security [14][15]. The implementation of security frameworks such as OWASP and NIST SP 800-115 not only provides a solid structure for conducting security assessments of educational institution websites but also provides practical guidance for mitigating identified risks [16][17].

The use of assessment tools such as Acunetix Vulnerability Scanner, NMAP, Nikto, Wireshark, and Nessus have shown significant effectiveness in identifying various levels of system vulnerabilities, from the network to the application level [18][19][20]. This combination of tools allows for a thorough examination of the security aspects of a website, including response header analysis, SSL/TLS security testing, and server configuration evaluation [21][12]. This multi-tool approach also facilitates cross-validation of findings and improves the accuracy of security assessments, resulting in a more comprehensive picture of the system's security posture [6][22].

Previous research on e-learning system security and academic repositories has revealed that cyber-attacks on educational institutions are increasingly complex and potentially impactful [23][24]. Vulnerability analysis of various online educational platforms shows the evolution of increasingly sophisticated and diverse attack patterns, which require a more adaptive and responsive security approach [5][25]. The implementation of a structured security framework, combined with regular assessments, has proven effective in improving the security posture of educational institutions and preventing vulnerability exploitation [8][16].

Based on the complexity of the challenges, this research proposes the application of a systematic and comprehensive Vulnerability Assessment method on the website of a college in Malang, Indonesia by integrating various continental security

tools and frameworks [15][8][18]. This approach not only aims to identify existing vulnerabilities but also to develop effective mitigation strategies and practical recommendations to improve system security [22][17]. The results of this study are expected to provide a significant contribution to the development of a more effective security model for higher education institutions in Indonesia, as well as being a reference for implementing best security practices in the education sector.

2. LITERATURE REVIEW

The increasing complexity and frequency of cyber-attacks on academic websites have driven extensive research on security analysis methods. As educational institutions increasingly rely on digital platforms to manage learning and administrative processes, ensuring the security of these systems becomes paramount. One of the most effective approaches to identifying and mitigating potential security threats is vulnerability assessment, which has been widely recognized as a crucial step in safeguarding academic information systems.

Saputra et al.emphasized the importance of comprehensive security evaluation techniques to protect academic information systems [26]. Their research identified prevalent threats, such as SQL Injection, Path Traversal, and improper server configurations. These vulnerabilities, if left unaddressed, could compromise the confidentiality, integrity, and availability of critical academic data. To mitigate these risks, the authors proposed strategic recommendations, including enhancing input validation mechanisms and strengthening server security configurations.

Aziz conducted a vulnerability assessment on an e-learning application, revealing several security holes that posed significant risks [4]. These vulnerabilities had the potential to expose sensitive user data and disrupt educational services. The findings underscored the necessity of adopting proactive measures to fortify e-learning platforms against cyber threats.

Budiman et al. highlighted the need for comprehensive assessments to bolster the security posture of academic websites [3]. Their study focused on addressing vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS), both of which are common attack vectors targeting web applications. Through meticulous evaluation and remediation efforts, educational institutions can significantly reduce the likelihood of security breaches.

Riadi et al. examined the security of an open journal system, identifying several weaknesses that attackers could exploit [2]. The researchers recommended implementing robust input validation techniques and secure server configurations to mitigate these vulnerabilities. Their findings demonstrated that even widely used academic systems require constant security monitoring and updates to maintain resilience against evolving threats.

Similarly, Aslan et al.conducted a comprehensive review of cyber threats targeting educational platforms [5]. Their research highlights how malicious actors can exploit vulnerabilities in system design and implementation.. They advocated for adopting robust security solutions, including continuous vulnerability assessments and integrating advanced threat detection mechanisms.

Liao et al. explored the application of vulnerability assessment methods in securing Internet of Things (IoT) devices within educational environments [6]. As IoT technologies become more prevalent in education, securing these connected systems is critical. Liao et al. concluded that regular security reviews are essential to maintaining a safe and secure environment for both students and faculty members.

Furthermore, Supriadi et al.emphasized the importance of adhering to OWASP (Open Web Application Security Project) standards in enhancing website security for educational institutions [8]. Their study demonstrated that vulnerability assessment frameworks based on OWASP guidelines provide practical tools for identifying and mitigating security risks. By leveraging these frameworks, educational institutions can better protect their digital assets.

Putri reinforced this perspective by highlighting the benefits of structured vulnerability assessments [9]. Her research showed how these assessments can effectively pinpoint configuration issues and potential threats within website management systems, enabling institutions to implement timely and appropriate remediation strategies.

In conclusion, the literature underscores the critical role of vulnerability assessments in safeguarding academic information systems. By identifying and addressing security weaknesses, educational institutions can maintain system integrity, protect sensitive data, and foster a secure digital ecosystem. The adoption of comprehensive and up-to-date security practices remains a vital priority for educational organizations seeking to navigate the dynamic landscape of cybersecurity threats..

3. RESEARCH METHODOLOGY

This study uses the Vulnerability Assessment method to analyze the security of the website of one of the colleges in Malang, Indonesia. This method was chosen because it can identify, evaluate, and provide recommendations on potential security vulnerabilities in the system. The research process involves several main interrelated stages, which can be seen in Figure 1. This approach builds upon insights from prior research, highlighting the

necessity of a comprehensive assessment strategy to detect and address vulnerabilities effectively [26].

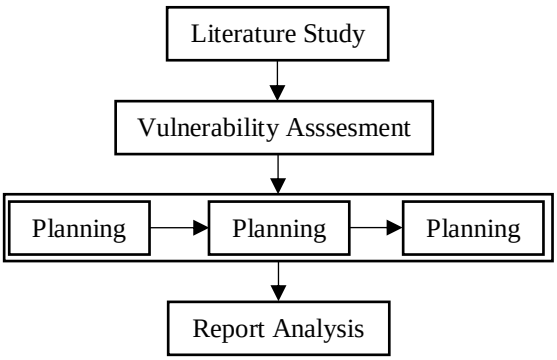

Figure 1. Research thinking framework

This research process begins with a literature study to collect various relevant information and references related to the concept of website security, vulnerability assessment techniques, and supporting tools to be used. This stage aims to provide a strong theoretical basis for designing further research steps.

The main stages of research begin with the Vulnerability Assessment process, which includes three steps: planning, scanning, and reporting [2]. The first step, planning, focuses on initial planning, including defining the scope of the analysis, setting research objectives, and selecting the tools and resources to be used. This stage aims to ensure that the research is directed and efficient.

The second step is scanning, where a thorough scan is performed on the website using tools such as Acunetic, OWASP ZAP, or similar tools. This process aims to detect security vulnerabilities, such as SQL injection holes, cross-site scripting (XSS), or system misconfigurations. The results of this scanning process are data vulnerabilities found on the system, including details of the type and severity. The functions and tools used in the planning and scanning stages are shown in Table 1.

Table 1. Stages, functions, and tools used

Stages	function	Tools
Planning	Domain info	Whois
	Port, scanning service detection and network info	Nmap
	View devices or sevices exposed on the internet	Shodan
Scanning	Web scanner vulnerability	Acunetix
	Cheking web application vulnerabilities XSS, SQL, Injection, CSRF	Owasp zap

The third step, reporting, is the process of preparing an initial report containing the results of the evaluation of the previous stages. This report includes information about the vulnerabilities found to lead to preventive measures and system improvements. This process aims to provide guidance that can be used by college website managers to improve the security of their systems.

The final stage of the research analysis is the report, which provides a comprehensive overview of the security condition of the website. Based on the results of the analysis, the main findings in the form of types of vulnerabilities are formulated, followed by specific recommendations for improvement. Thus, the report produced is not only intended to provide theoretical insights but also provides practical solutions that can be applied by website managers to significantly improve the security of their systems.

4. RESULT AND DISCUSSION

4.1. Planning

At the planning stage, researchers collect initial information related to the website that is the object of research, namely information related to websites at universities. At this planning stage, the researcher carried out 3 stages, the first was the implementation of the use of Whois, the second stage was the implementation of Nmap, and the third stage was the implementation of the use of Shodan.

4.1.1. Whois

The use of Whois is useful for searching for information related to domains, in this stage aims to identify technical details such as domain information analysis, information registration status, IP addresses, and other basic configurations relevant to security. The results of the implementation of Whois can be seen in Figure 2.

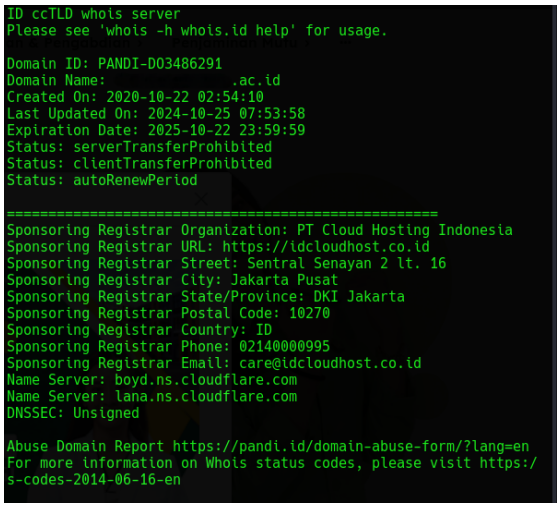

Figure 2. Whois implementation

Based on Figure 2, Whois lookup analysis was performed to obtain information related to the domain xxxx.ac.id. The results of the analysis show several key pieces of information, namely: Domain ID: PANDI-D03486291, with the registrar PT Cloud Hosting Indonesia, located at Sentral Senayan 2 Lt. 16, Central Jakarta, DKI Jakarta, Indonesia. This registrar provides services through the official

website https://idcloudhost.co.id, email care@idcloudhost.co.id, and telephone number 02140000995. The domain xxxx.ac.id was first registered on October 22, 2020, at 02:54: 10 WIB, with the last update being made on October 22, 2024, at 07:53:58 WIB, and valid until October 22, 2025, at 23:59:59 WIB.

This domain has a status of client Transfer Prohibited, indicating that the domain is protected from unauthorized transfers, and a status of auto Renew Period, indicating that the domain is in an automatic renewal period. The name servers used are lana.ns.cloudflare.com and boyd.ns.cloudflare.com, while the DNSSEC security mechanism has not been implemented with the status unsigned. The information obtained from this Whois lookup is very important for validating domain ownership, ensuring the domain's active status, and transmitting the security mechanisms implemented, such as DNSSEC. It also serves to identify the registrar responsible for managing the domain.

4.1.2. Nmap

The use of Nmap is useful for finding information related to network mapping. This network mapping stage aims to find information related to ports and services that are active on the university website domain. The results of the Nmap implementation can be seen in Figure 3.

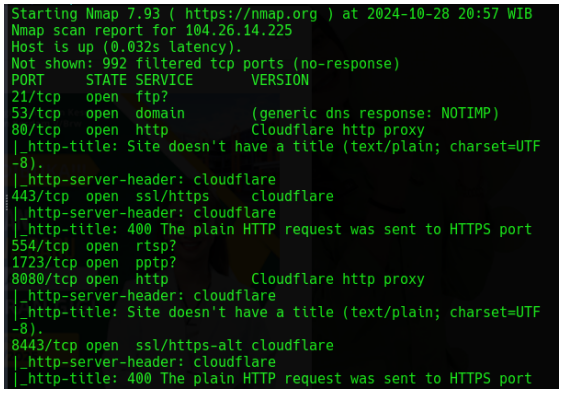

Figure 3. Nmap implementation

Based on the results shown in Figure 3, several ports are open on the server with the IP address 104.26.14.225, indicating certain services. Port 21/tcp is detected as an active FTP (File Transfer Protocol) service, indicating server support for file transfers. Port 53/tcp indicates the presence of a DNS (Domain Name System) service, which is used to manage domain name resolution. Furthermore, ports 80/tcp and 8080/tcp indicate an HTTP service running through the Cloudflare proxy, which functions to improve the performance and security of web connections. In addition, ports 443/tcp and 8443/tcp indicate the presence of an HTTPS (Secure HTTP) service that also uses Cloudflare as a proxy, providing encryption on connections to protect user data. Another detected port is 554/tcp, indicating an RTSP (Real-Time Streaming Protocol) service, possibly used to support real-time data streaming services. Meanwhile, port 1723/tcp is detected as PPTP (Point-to-Point Tunneling Protocol) service, which is usually used to support Virtual Private Network (VPN) connections.

The results of this analysis show that the server has a few services managed with Cloudflare support to improve performance and security. However, the presence of open ports, especially for FTP and PPTP, can be a potential security risk that needs to be further evaluated. This analysis provides a comprehensive picture of the services running on the server and is an important basis for maintaining overall network security.

4.1.3. Shodan

Shodan is useful tool for viewing devices or services exposed on the internet. Shodan allows researchers to access a variety of important information. This information includes hosts and IP addresses, open ports and running services, system configurations and protocols, SSL/TLS certificates, security vulnerabilities (CVEs - Common Vulnerabilities and Exposures), IoT devices and SCADA systems, passive analysis, domain crawling, and network infrastructure management and monitoring.

Search results using Shodan on the college website link show that the server uses Apache as the main web server with HTTPS protocol support through an SSL certificate issued by Let's Encrypt. The HTTP response given shows a status code of 301 Moved Permanently, which redirects the request to a more secure URL. This server also supports the latest security protocols, such as TLSv1.3, to ensure the security of encrypted communications. Based on geolocation information, this server is in Jakarta, Indonesia, and is registered under the organization PT. Halto Petra Argowiyata, with support from the internet service provider PT Cloud Hosting Indonesia.

Additionally, port checking shows that port 80 (HTTP) is open and active. The server returns an HTTP 200 OK response, with a combination of using the Apache web server and a nginx-based view. The server supports the HTTP/2 protocol, and the HTTP headers provide additional information, such as ETag and Last-Modified, indicating the use of caching mechanisms to improve data access efficiency. However, even though HTTPS support is available, the use of the HTTP port (without encryption) can be a potential point of vulnerability if no automatic redirection to HTTPS is performed.

The analysis also shows that this server is connected to the cloudhost.web.id domain, which operates from the Rengasdengklok area, Indonesia. The information obtained highlights the importance of evaluating hosting infrastructure to detect

potential security weaknesses, especially in protocol management, open ports, and data security mechanisms. The presence of open HTTP ports can be a serious concern, considering the potential for threats such as Man-in-the-Middle (MITM) attacks on unencrypted connections. Using Shodan, this study shows how passive analysis of a system can provide deep insights into network configurations, security risks, and mitigation steps needed to improve cyber resilience.

4.2. Scanning

At this stage, a scanning process is carried out to identify weaknesses or vulnerabilities in the system that is the object of research. The scanning process uses software vulnerability assessments that automatically check components, configurations, and protocols in the system to detect potential threats. At this stage, researchers use Acunetix and OWASP ZAP Top 10.

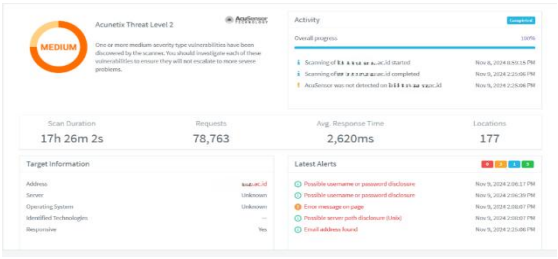

Figure 4. Acunetix implementation

Based on the scanning results shown in Figure 4, the website domain at the university is at level 2 (Medium). This indicates the presence of one or more vulnerabilities with a medium risk level, so it needs to be checked immediately so that it does not develop into a more serious problem. Some of the vulnerabilities identified in the report include the possibility of disclosing credentials, such as usernames or passwords, with two detected incidents. In addition, error messages were also found that were visible on the web page, the potential for spreading server paths on Unix-based systems, and the discovery of email addresses that could be used by unauthorized parties. The results of this test underline that although the web system on the domain shows good responsiveness, there are still potential vulnerabilities that require further mitigation steps to increase its security level.

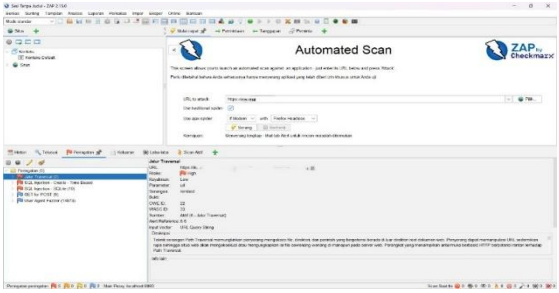

Figure 5. OWASP implementation

The results of scanning university website links using OWASP ZAP Top 10 are shown in Figure 5. Based on this, 5 vulnerabilities were detected, including traversal path, sql injection-Oracle-time based, sql injection-sqllite, get for post, and the last is user agent fuzzer. These five vulnerabilities are explained in the next sub-chapter.

4.3. Reporting

The reporting stage aims to present information related to identified vulnerabilities. The results of this stage are in the form of alerts regarding vulnerabilities, risk levels classified as high, medium, low, and additional information. The results are presented in Table 2, which displays a report of the results of testing the university website. The test identified five threats with the number of risks categorized as high, medium, low, and information.

Table 2. Vulnerability testing result

Alert	Risk			
	High	Medium	Low	Information
Path traversal	2			
Sql injection – time based	2			
Sql injection – sqlite	10			
Get for post				9
User agent fuzzer				14873

Path Traversal, also known as Directory Traversal, is an attack that aims to access files and directories located outside the web root folder. This attack usually occurs due to the system's inability to restrict pathname access to the specified directory. This risk falls into the High category with two identified incidents. This vulnerability can be exploited to gain unauthorized access to sensitive information that should not be accessible to external users..

Time-based SQL Injection is a form of attack where the perpetrator exploits vulnerabilities in the Oracle database. By manipulating SQL commands through unvalidated user input, attackers can obtain sensitive data or alter the application's behavior. This risk is recorded at a high level, with two incidents successfully identified. Time-based SQL Injection allows the perpetrator to determine the server's response based on the time it takes to execute a specific command, indicating that the database has been successfully exploited.

SQL Injection on SQLite is a variant of attack that exploits weaknesses in the management of SQL commands by the SQLite database. This attack allows the attacker to inject malicious SQL commands that can expose, alter, or even delete important data within the database. This risk falls into the High category, with ten identified incidents.

This type of SQL Injection often occurs due to the lack of user input validation or proper sanitization mechanisms.

This vulnerability occurs when an HTTP request that should be sent as a POST method can also be accepted by the server using the GET method. Although this condition is not directly considered a security vulnerability, it can facilitate further attacks, such as Cross-Site Scripting (XSS). For example, accepting a similar GET request can simplify the attack if a POST request is vulnerable to XSS. This risk has a Medium level, with nine identified incidents.

User Agent Fuzzer is a security testing method that examines the differences in server responses based on modified User Agents, such as access through mobile sites or search engine crawlers. This technique compares the response status and hash code of the original response content with the response given for the modified User Agent. This finding may indicate a weakness in server response management, which attackers could exploit. This vulnerability has an incident count of 14,873 and falls into the Information risk category.

4.4. Recommendation

Based on the results of the security analysis that has been carried out, it is recommended that university website managers routinely update the software, frameworks, and libraries used to address vulnerabilities such as SQL Injection, Path Traversal, and potential user data disclosure. The use of the HTTPS protocol with the latest version of TLS is very important to protect data from threats such as Man-in-the-Middle (MITM), while the implementation of Content Security Policy (CSP) can prevent Cross-Site Scripting (XSS) attacks. In addition, server configuration must be strengthened by closing unnecessary ports, such as FTP and PPTP, and ensuring that only relevant services are running on the server. Elimination of error messages that expose sensitive information also needs to be done to reduce the risk of exploitation. Periodic security audits using frameworks such as OWASP and NIST SP 800-115 are highly recommended to ensure that the system remains protected from new vulnerabilities. Tools such as Acunetix, OWASP ZAP, and Nmap can be used to support this audit process by providing accurate results.

On the policy side, system managers need to implement role-based access control (RBAC) to restrict access based on user roles and adopt multi-factor authentication (MFA) to protect user accounts from unauthorized access. Regular cybersecurity training is also needed to increase staff awareness of cyber threats and mitigate them. Furthermore, the installation of a log-based monitoring system and anomaly analysis can detect suspicious activity in real time. Integrating the system with a threat detection platform, such as SIEM (Security Information and Event Management), can provide faster response capabilities to security incidents. By implementing these steps, it is hoped that the security level of the X campus website in Malang City can be significantly improved, thereby protecting sensitive data and ensuring the continuity of digital services safely.

5. CONCLUSION

This study has analyzed the security website of a college located in Malang, Indonesia using the Vulnerability Assessment method, which includes the Planning, Scanning, and Reporting stages. Based on the results of the study, several security vulnerabilities were found, including SQL Injection, Path Traversal, sensitive data disclosure, and weaknesses in server configuration. The risk levels of the identified vulnerabilities vary from high, medium, low, indicating that even though the system has several protection mechanisms, there is still significant potential for exploitation. The method used in this study has proven effective in identifying vulnerabilities at various levels of the system, including web applications and server infrastructure. Tools such as Acunetix, OWASP ZAP Top 10, and Nmap make a major contribution to detecting security vulnerabilities with high accuracy, while security frameworks such as OWASP and NIST SP 800-115 serve as strong guides in implementing the assessment process.

Based on these findings, it is concluded that implementing mitigation measures, such as regular software updates, strengthening server configurations, implementing the latest security protocols, and regular security audits, are essential to improving the security posture of a website. In addition, system managers are advised to adopt role-based security policies (role-based access control) and increase security awareness through regular training. Implementation of a log-based monitoring system and integration with a threat detection platform are also needed to support real-time cyber threat detection and response. This study provides an important contribution to the development of website security models in higher education, especially in the context of increasingly complex cyber threats. The findings and recommendations produced can be a reference for system managers in improving digital security and protecting sensitive data. In the future, it is hoped that similar research can be conducted with a wider scope, including analysis of various types of educational information systems, to provide a more comprehensive insight into cybersecurity in the education sector.

REFERENCES

[1] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, “Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case

Studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021, doi: 10.1109/ACCESS.2021.3058403.

[2] I. Riadi, A. Yudhana, and Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 4, pp. 853–860, Aug. 2020, doi: 10.25126/jtiik.2020701928.

[3] A. Budiman, S. Ahdan, and M. Aziz, "ANALISIS CELAH KEAMANAN APLIKASI WEB E-LEARNING UNIVERSITAS ABC DENGAN VULNERABILITY ASSESMENT," *J. Komputasi*, vol. 9, no. 2, pp. 1–10, Oct. 2021, doi: 10.23960/komputasi.v9i2.2800.

[4] M. A. Aziz, "VULNERABILITY ASSESMENT UNTUK MENCARI CELAH KEAMANAN WEB APLIKASI E-LEARNING PADA UNIVERSITAS XYZ," *J. Eng. Comput. Sci. Inf. Technol.*, vol. 2, no. 1, Mar. 2023, doi: 10.33365/jecsit.v1i1.13.

[5] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.

[6] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020, doi: 10.1109/ACCESS.2020.3006358.

[7] A. S. Alif Muhammad Akmal, Nono Heryana, "Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment," *Comput. Secur.*, vol. 89, no. 4, p. 101666, Feb. 2020, doi: https://doi.org/10.31004/jpdk.v4i4.6495.

[8] D. Supriadi, E. Suryadi, R. Muslim, and L. D. Samsumar, "IMPLEMENTASI VULNERABILITY ASSESSMENT OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA WEBSITE UNIVERSITAS TEKNOLOGI MATARAM," *J. Data Anal. Information, Comput. Sci.*, vol. 1, no. 4, pp. 232–240, Oct. 2024, doi: 10.70248/jdaics.v1i4.1368.

[9] D. E. Putri, "VULNERABILITY ASSESSMENT PADA WEBSITE PORTAL MANAJEMEN INFORMATIKA POLITEKNIK LP3I," *Bull. Netw. Eng. INFORMATICS*, vol. 1, no. 2, p. 42, Oct. 2023, doi: 10.59688/bufnets.v1i2.11.

[10] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," *J. Inf. dan Teknol.*, vol. 89, no. 1, pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.

[11] S. C. . Yusuf Muhyidin, M. Hafid Totohendarto, Erina Undamayanti, "Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking," *Comput. Secur.*, vol. 89, no. 1, p. 101666, Feb. 2020, doi: https://doi.org/10.51132/teknologika.v12i1.143.

[12] F. Kristianto, S. Rahman, and S. Bahri, "ANALISIS KERENTANAN PADA WEBSITE SERVIO MENGGUNAKAN ACUNETIX WEB VULNERABILITY," *JTRISTE*, vol. 9, no. 1, pp. 46–55, Mar. 2022, doi: 10.55645/jtriste.v9i1.363.

[13] W. Wahyudin, H. Kuswara, R. Resti, and S. Dalis, "Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website Points of Sales," *Comput. Sci.*, vol. 4, no. 1, pp. 44–52, Jan. 2024, doi: 10.31294/coscience.v4i1.2978.

[14] D. Upadhyay and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations," *Comput. Secur.*, vol. 89, p. 101666, Feb. 2020, doi: 10.1016/j.cose.2019.101666.

[15] A. S. Syahab, E. I. H. Ujianto, and R. Rianto, "PENGGUNAAN WIRESHARK DAN NESSUS UNTUK ANALISIS SSL/TLS PADA KEAMANAN DATA PENGGUNA WEBSITE," *JIKA (Jurnal Inform.*, vol. 7, no. 2, p. 183, May 2023, doi: 10.31000/jika.v7i2.7566.

[16] E. Z. Darojat, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," *J. Sist. Inf. BISNIS*, vol. 12, no. 1, pp. 36–44, Sep. 2022, doi: 10.21456/vol12iss1pp36-44.

[17] C. Darmawan, J. P. P. Naibaho, and A. De Kweldju, "Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021," *Edumatic J. Pendidik. Inform.*, vol. 8, no. 1, pp. 272–281, Jun. 2024, doi: 10.29408/edumatic.v8i1.25834.

[18] A. Rochman, rizal R. Salam, and S. A. Maulana, "Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit Xyz," vol. 2, no. 4, p. 6, 2021, doi: https://doi.org/10.59141/jist.v2i04.124.

[19] Riyan Farismana and Dian Pramadhana, "Perbandingan Vulnerability Assesment Menggunakan Owasp Zap dan Acunetix Pada Sistem Informasi Repositori Politeknik Negeri Indramayu," *J. Tek. Inform. dan Teknol. Inf.*, vol. 3, no. 2, pp. 26–32, Aug. 2023, doi: 10.55606/jutiti.v3i2.2853.

[20] Riyan Farismana and Dian Pramadhana, "VULNERABILITY ASSESSMENT UNTUK ANALISIS TINGKAT KEAMANAN PADA SISTEM INFORMASI REPOSITORI KARYA ILMIAH POLITEKNIK NEGERI INDRAMAYU," *J. Tek. Inform. dan Teknol. Inf.*, vol. 3, no. 1, pp. 26–33, Apr. 2023, doi: 10.55606/jutiti.v3i1.2208.

[21] H. Kurniawan and E. Christianto, "Analysis Vulnerability Website Baleomolcreative dengan Metode Penetration Testing Execution Standard & Vulnerability Assessment Pada Http Response Header Field," *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 8, no. 3, pp. 734–745, Jul. 2024, doi: 10.35870/jtik.v8i3.2202.

[22] S. A. Hafsari and H. Harjono, "Analisis Keamanan Website Pendaftaran Mahasiswa Baru Dengan Munggunakan Metode Vulnerability Assessment," *TIN Terap. Inform. Nusant.*, vol. 4, no. 11, pp. 698–708, Apr. 2024, doi: 10.47065/tin.v4i11.5060.

[23] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *Int. J. Inf. Secur.*, vol. 21, no. 1, pp. 115–158, 2022, doi: 10.1007/s10207-021-00545-8.

[24] Rifky Lana Rahardian, "ANALISIS KEAMANAN WEB NEW KUTA GOLF MENGGUNAKAN METODE VULNERABILITY ASSESSMENTS DAN PERHITUNGAN SECURITY METRIKS," *J. Inform. Dan Tekonologi Komput.*, vol. 2, no. 3, pp. 256–265, Nov. 2022, doi: 10.55606/jitek.v2i3.582.

[25] Mira Orisa and M. Ardita, "VULNERABILITY ASSESMENT UNTUK MENINGKATKAN KUALITAS KEMANAN WEB," *J. Mnemon.*, vol. 4, no. 1, pp. 16–19, Feb. 2021, doi: 10.36040/mnemonic.v4i1.3213.

[26] D. W. Saputra, R. S. Pradini, and M. Anshori, "Analisis dan Rekomendasi Keamanan Website Kampus X Menggunakan ISSAF," *J. Indones. Manaj. Inform. dan Komun.*, vol. 6, no. 1, pp. 830–843, Jan. 2025, doi: 10.35870/jimik.v6i1.1306.