Research Article

International Journal of Information System and Technology (IJOINT)
Volume 01, Issue 02, PP. 44–51

Website Security Analysis Using Penetration Testing

Anugrah Utama [1*], Khairil [2], and Reno Supardi [3]
[1] Student, Faculty of Computer Science, Dehasen University, Bengkulu, Indonesia
Email: anugurah.utama45@gmail.com [1]
[2,3] Lecture, Faculty of Computer Science, Dehasen University, Bengkulu, Indonesia
Email: khairil@unived.ac.id [2], trenosupardi00@gmail.com [3]

*Corresponding Author Email: anugurah.utama45@gmail.com

Received: January 15, 2025; Revised: January 29, 2025; Accepted: February 15, 2025

Abstract

Websites are a vital element in the evolution of the internet, with more than 1.9 billion sites worldwide today. Their use was initially limited to personal purposes, but now almost every company has a website, such as Facebook, Apple, and BBC News. Tim Berners-Lee created the first website in the late 1980s through the World Wide Web (W3) project. Penetration Testing is an evaluation method to identify weaknesses in the security of a system, network, or web application. It involves a direct attack on the target being tested to detect and fix weaknesses. The goal is to identify potential weak points and ensure compliance with security policies. The test results using Accuntetix showed a low-level system vulnerability on the min2kotabengkulu.sch.id website, which can be considered quite safe from attacks.

Keyword: PENTEST, Security, Website, Accuntetix

1. Introduction

The development of information technology today has grown very rapidly. The need to obtain information quickly requires us to utilize the information technology that is currently available (Mehmood, 2021). Information is very valuable in this era of globalization. Since the presence of the internet, information is no longer limited. The use of information and communication technology today has become an effective and efficient way to convey information to the public (Szymkowiak et al., 2021); (Wang et al., 2021). In recent decades, the development of information technology has changed the way organizations operate and interact with customers (Rosário & Raimundo, 2021). Websites, as one of the main elements in digital transformation, have become the backbone of many businesses, government agencies, and other organizations (Mohamed Hashim et al., 2022); (West, 2019). However, along with the increasing dependence on websites, cyber security threats are also increasingly complex and diverse (Jang-Jaccard & Nepal, 2014); (Renaud & Coles-Kemp, 2022). According to reports from various cyber security agencies, cyberattacks such as SQL Injection, Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS), and phishing continue to increase both in frequency and sophistication (Kaur et al., 2023); (Rodríguez et al., 2020).

Website security is not just about protecting data, but also about maintaining business continuity and user trust (Flavián & Guinalíu, 2006). A secure website can prevent cyberattacks, ensure service availability, and protect sensitive information such as customer personal data, financial transactions, and business secrets (Aslan et al., 2023); (Miracle, 2024). In addition, website security is also an important factor in meeting regulatory requirements and industry or organizational security standards (Mirtsch et al., 2020). Madrasah Ibtidaiyah Negeri 2 Kota Bengkulu has used the Web as a means of publication related to educational

activities and a means of conveying information to parents. Given the importance of the data contained therein, it is necessary to implement security testing of the Publication Website.

To address cyber threats, organizations need to take a proactive approach to managing information security. One effective method is to conduct penetration testing (Pentest) (Aboelfotoh & Hikal, 2019); (Shah & Mehtre, 2013). Penetration testing is a controlled process of simulating a cyberattack to identify vulnerabilities in a system, network, or application. By conducting this testing, organizations can not only protect their digital assets but also ensure business continuity, comply with regulations, and maintain customer trust (Knowles et al., 2016); (Stiawan et al., 2017). Therefore, penetration testing is not only a preventive measure, but also a long-term investment in the security and sustainability of the organization.

2. The Art of Research

Penetration Testing is an assessment method by testing the weaknesses of system security, computer networks or web application program weaknesses (Shah & Mehtre, 2013). By conducting direct attacks on the target or system to be tested. The results of this test can be input to improve the weaknesses of the detected system, so as to improve security and to avoid cyberattacks. The PTES phase is designed to explain a Penetration Testing and ensure the client that a standardization level effort consisting of 7 measurement phases (Sarker, 2023) (see figure 1).

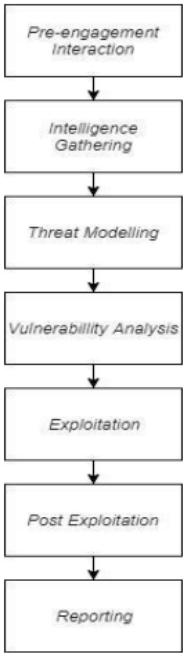

Figure 1. Penetration Testing Execution Standard

The initial stage of the research will begin with pre-engagement interaction in the form of information exchange and test plans, followed by the intelligence gathering phase which aims to find as much information as possible in the penetration process later (vulnerability assessment and exploitation phase). The next phase is threat modeling which is a procedure for optimizing network security by identifying objectives and weaknesses, and determining countermeasures to prevent system vulnerabilities. The next stage is called the vulnerability testing stage which is carried out as a process to find a weakness in the system and applications that can be used. The next stage is called the exploitation stage which focuses on establishing access to a system by bypassing security restrictions. The next stage will be carried out the post-exploitation

stage to determine the price of the system and to maintain control of the system so that it can be used later. The last is to write a report that describes the complete results of the test and the presentation that has been prepared with recommendations and solutions.

3. Method

This research is an experimental research method. This method is validation or testing, namely identifying weak points on the Web of Madrasah Ibtidaiyah Negeri 2 Kota Bengkulu. The analysis of the actual system on the running system will be carried out in this study using several supporting software as presented in table 2 and for the penetration testing strategy using the White Box Testing strategy, namely where the tester has access to obtain all the information needed transparently.

Table 2. Details of Software Used

No	Software Analysis	Tools
1	Web Server	Litespeed
2	Database	MySQL 5.1.1
3	Programming	PHP 7.2.36
4	CMS	Wordpress 6.1.1
5	SSL	Let's Encrypt
6	Plugin	Elementer Pro
7	Themes	Crcote Corporate

4. Result

1. Pre-engagement Interaction

At this stage, the author confirmed with the website administrator and asked for permission to conduct Penetration Testing on the min2kotabengkulu.sch.id website which is managed by the school admin as a place for promotion, sharing information and student registration for the school.

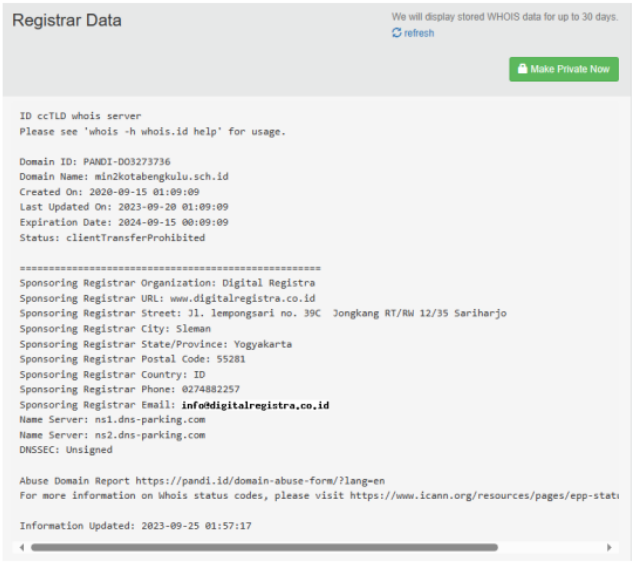

Figure 2. Results of Collecting Initial Website Information Through the WhoIs Page

2. Intelligence Gathering

The Intelligence Gathering stage is carried out by collecting information on websites that obtain some website information with a scanning process using whois and obtain some information starting from the time the domain was created, the domain expired, where the domain was registered and the client status Transfer

Prohibited where the domain is not allowed to be transferred to another registrar or is not allowed to carry out DNS Zone Transfer (see figure 2). Furthermore, for the scanning results using Zenmap with profile instance, all TCP ports show the server information used, namely LiteSpeed hosting used, namely Hostiger and several detected ports are left open (see figure 3 and table 3) for system access.

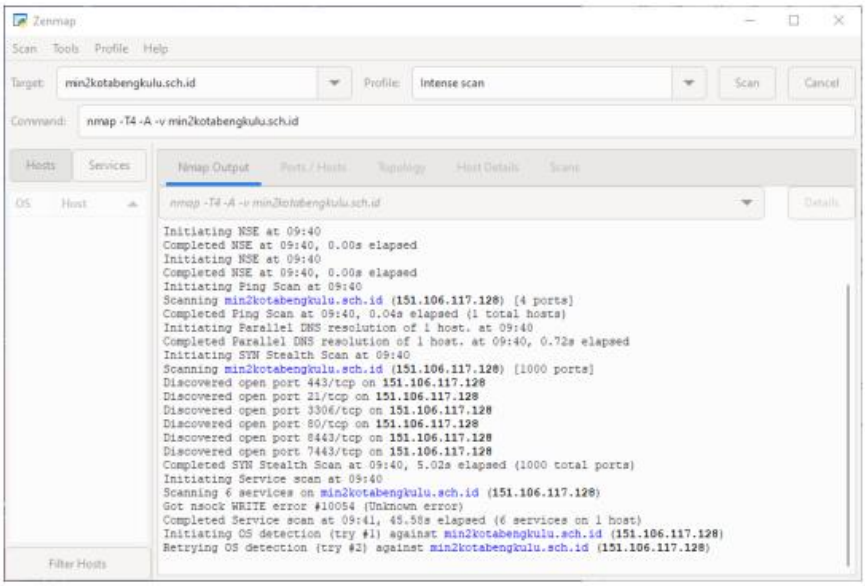

Figure 3. Website Information Search Results Using Zenmap GUI

Table 3. Zenmap scanning results with Intense Profile

Scanning Result	Information
Server	LiteSpeed
Platform	Hostiger
port 443/tcp on 151.106.117.128	Open
port 21/tcp on 151.106.117.128	Open
port 3306/tcp on 151.106.117.128	Open
Port 80/tcp on 151.106.117.128	Open
Port 8443/tcp on 151.106.117.128	Open
Port 7443/tcp on 151.106.117.128	Open

3. Vulnerabillity Analysis

This stage begins by scanning the website using the Accunetix tools and on the scan information dashboard (see Figure 4) there is information that the scanning results show potential system vulnerabilities at a low level and there are several system vulnerability warnings in the Latest Alerts section.

The results of further scanning using Accunetix software showed that the website being tested had 3 vulnerabilities at the low level and 3 informational warnings (see table 4) which showed that the position of the website server was still in the safe category with the statement that there were no vulnerabilities at the medium or hard level.

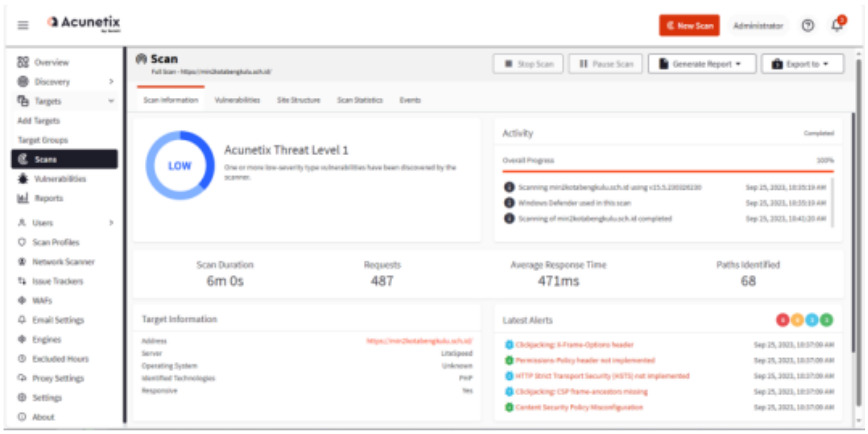

Figure 4. Scanning Results Using Acunetix Software

4. Exploitation

SQL Injection is a security attack technique on web applications that allows attackers to inject malicious SQL code into input expected by the application. This can lead to unauthorized manipulation or access to the database, as well as the execution of malicious SQL commands. From the results of the scanning test using Accunetix, no security holes were found in the form of SQL Injection, therefore the exploitation process using SQLmap was not carried out.

Table 4. Accunetix Scanning Results and News Alerts

Types of Vulnerabilities	Total	Vulnerability Level
Clickjacking: CSP frame-ancestors missing	2	Low
HTTP Strict Transport Security (HSTS) not implemented	1	Low
Content Security Policy Misconfiguration	1	Information
PHP Version Disclosure	1	Information

5. Reporting

At the reporting stage, all data from the test results are collected into a report. Starting with a surveillance report using whois and continuing through scanning using zenmap which ends with penetration through accunetix software, several vulnerabilities were found at several levels of the website. At the Exploitation stage, it was not carried out because no security holes were found in the form of SQL Injection when scanning with Accunetix was completed, so the website was safe from SQL Injection.

5. Discussion

At the exploitation stage, several security holes were found on the min2kotabengkulu.sch.id website, including: One, Clickjacking: CSP frame-ancestors missing, which is an attack technique by inserting web pages in transparent frames on fake websites. The way to overcome this is to limit how web pages can be loaded in frames (Weissbacher et al., 2014). The methods that can be used by system security admins to handle Clickjacking are to set the X-Frame-Options header in the web server settings with the value "deny" or "sameorigin". Second, Permissions-Policy Header Not Implemented, which allows you to control various permissions on web pages, such as camera access, microphone, and others. Implementing Permissions-

Policy can help mitigate security risks (Lathifah et al., 2022). The methods that can be used by system security admins to handle Permissions-Policy are to set the Permissions-Policy header in the web server settings according to specific needs.

Third, HTTP Strict Transport Security (HSTS) Not Implemented, where HSTS is a security mechanism that forces clients (such as browsers) to always use HTTPS when connecting to certain websites in order to reduce the risk of MITM attacks (Sebrina et al., 2024). The methods that can be used by system security admins to handle HTTP Strict Transport Security (HSTS) Not Implemented are by enabling HSTS on the server, setting the Strict-Transport-Security header with the appropriate value and ensuring that the website can only be accessed via HTTPS. Fourth, Clickjacking: CSP Frame-Ancestors Missing where Content Security Policy (CSP) is a mechanism that allows websites to limit the resources that can be loaded on their pages. Frame-Ancestors is a directive in CSP that limits which pages can load pages in frames (Roth et al., 2020). The methods that can be used by system security admins to handle Clickjacking: CSP Frame-Ancestors Missing are by implementing CSP on the website and adding the frame-ancestors directive to the CSP header.

6. Conclusion

Penetration testing research conducted on the school website aims to identify security vulnerabilities that may be exploited by irresponsible parties. Based on the test results, several security holes were found, such as Clickjacking: CSP frame-ancestors missing, Permissions-Policy Header Not Implemented, HTTP Strict Transport Security (HSTS) Not Implemented and Clickjacking: CSP Frame-Ancestors Missing. These findings indicate that the school website is still in the safe category but is vulnerable to cyberattacks that can threaten the confidentiality, integrity, and availability of data. Vigilance is needed from representative actions taken by the system network security team.

Recommendations include implementing security patches, regular system updates, and security awareness training for website administrators. By fixing existing vulnerabilities, school websites can be more secure and protect sensitive data such as student information, teachers, and academic processes. Furthermore, this study recommends the importance of conducting routine penetration testing as part of a cybersecurity strategy to ensure the security and reliability of school information systems.

Although penetration testing research for school websites provides important insights into security vulnerabilities, there are several weaknesses including: One, Research may only focus on certain aspects of the website (e.g., web applications) without considering other components such as network infrastructure, databases, or integrated third-party systems. This can cause security vulnerabilities outside the scope of the study to go undetected. Two, Research may not be able to fully simulate real-world attacks due to ethical, legal, or technical limitations. For example, Distributed Denial of Service (DDoS) attacks are often not tested due to the risk of disrupting service.

Acknowledgments

-

References

1. Aboelfotoh, S. F., & Hikal, N. A. (2019). A review of cyber-security measuring and assessment methods for modern enterprises. JOIV: International Journal on Informatics Visualization, 3(2), 157-176.
2. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

3. Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. Industrial management & data Systems, 106(5), 601-620.
4. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993.
5. Kaur, J., Garg, U., & Bathla, G. (2023). Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review. Artificial Intelligence Review, 56(11), 12725-12769.
6. Knowles, W., Baron, A., & McGarr, T. (2016). The simulated security assessment ecosystem: Does penetration testing need standardisation?. Computers & Security, 62, 296-316.
7. Lathifah, A., Amri, F. B., & Rosidah, A. (2022, September). Security vulnerability analysis of the sharia crowdfunding website using owasp-zap. In 2022 10th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE.
8. Mehmood, T. (2021). Does information technology competencies and fleet management practices lead to effective service delivery? Empirical evidence from e-commerce industry. International Journal of Technology, Innovation and Management (IJTIM), 1(2), 14-41.
9. Miracle, N. O. (2024). The Importance of Network Security in Protecting Sensitive Data and Information. International Journal of Research and Innovation in Applied Science, 9(6), 259-270.
10. Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. IEEE Transactions on Engineering Management, 68(1), 87-100.
11. Mohamed Hashim, M. A., Tlemsani, I., & Matthews, R. (2022). Higher education strategy in digital transformation. Education and Information Technologies, 27(3), 3171-3195.
12. Renaud, K., & Coles-Kemp, L. (2022). Accessible and inclusive cyber security: a nuanced and complex challenge. SN Computer Science, 3(5), 346.
13. Rodríguez, G. E., Torres, J. G., Flores, P., & Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. Computer Networks, 166, 106960.
14. Rosário, A., & Raimundo, R. (2021). Consumer marketing strategy and E-commerce in the last decade: a literature review. Journal of theoretical and applied electronic commerce research, 16(7), 3003-3024.
15. Roth, S., Barron, T., Calzavara, S., Nikiforakis, N., & Stock, B. (2020, January). Complex security policy? a longitudinal analysis of deployed content security policies. In Proceedings of the 27th Network and Distributed System Security Symposium (NDSS).
16. Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods. Sustainability, 15(13), 10471.
17. Sebrina, A. F., Junaidi, A., & Sihananto, A. N. (2024). Testing posketanmu website with google penetration testing and OWASP Top 10. Jurnal Mantik, 8(1), 636-645.
18. Shah, S., & Mehtre, B. M. (2013). A modern approach to cyber security analysis using vulnerability assessment and penetration testing. International Journal of electronics communication and computer engineering, 4(6), 47-52.
19. Stiawan, D., Idris, M. Y., Abdullah, A. H., Aljaber, F., & Budiarto, R. (2017). Cyber-Attack Penetration Test and Vulnerability Analysis. International Journal of Online Engineering, 13(1).
20. Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., & Kundi, G. S. (2021). Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. Technology in Society, 65, 101565.
21. Wang, D., Zhou, T., & Wang, M. (2021). Information and communication technology (ICT), digital divide and urbanization: Evidence from Chinese cities. Technology in Society, 64, 101516.

22. Weissbacher, M., Lauinger, T., & Robertson, W. (2014). Why is CSP failing? Trends and challenges in CSP adoption. In Research in Attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden, September 17-19, 2014. Proceedings 17 (pp. 212-233). Springer International Publishing.
23. West, J. K. (2019). An introduction to online platforms and their role in the digital transformation. Available at SSRN 4669281.