System Security Testing Using The Penetration Testing Method on The Palapa Vocational School Library Website

Wawan Koswara1, Heni Sulistiani2, Surya Ramadhan3

[1] *Universitas Teknokrat Indonesia, Tulang Bawang, Indonesia*
[2] *Universitas Teknokrat Indonesia, Bandar Lampung, Indonesia*
[3] *Universitas Teknokrat Indonesia, Lampung Selatan, Indonesia*

Article Information

Received: 21-11-2024
Revised: 28-11-2024
Published: 05-12-2024

Keywords
Penetration Testing; SQL Injection; SQLmap; System Security; Website.

Correspondence Email:
Wawan_koswara2023@teknokrat.ac.id
Heni_sulistiani@teknokrat.ac.id
Surya_Ramadhan@teknokrat.ac.id

Abstract

The Palapa Library utilizes its website as the primary platform for providing information and services to users. However, the presence of vulnerabilities in the website poses significant threats to data and system security. This study aims to identify and analyze vulnerabilities on the Palapa Library website using the Penetration Testing method based on the NIST SP 800-115 standard. This method involves four stages: planning, discovery, attack, and reporting. The testing results identified two major vulnerabilities: sensitive information disclosure and SQL Injection. Once the vulnerabilities were identified, their severity levels were assessed using the Common Vulnerability Scoring System (CVSS) version 3.1. CVSS provides scores for the vulnerabilities, helping prioritize remediation efforts from the highest to the lowest risk. Based on the assessment results, appropriate remediation measures were developed to enhance the security of the Palapa Library website. This study is expected to serve as a reference for preventing similar security threats in the future and assisting other institutions facing similar challenges in improving the security of their information systems.

1. Introduction

The rapid development of information technology has brought significant changes in various fields, including the ease of access to information and digital services. One of the innovations that has emerged is the website, which is a collection of pages hosted on a domain or subdomain and can be accessed globally via the internet (Utama et al., 2022). With the presence of websites, information can be accessed more easily and quickly, ultimately supporting various daily activities.

At the Palapa Vocational School Library, the role of the website is crucial in providing information and digital learning resources for students and teaching staff. As a digital information center, the library has a web-based system designed to provide access to book collections, borrowing schedules, study guides, and other information related to library activities. Thus, the library's website facilitates the teaching and learning activities at Palapa Vocational School through effective access to digital information services.

However, based on a report received from a bug hunter, potential vulnerabilities were discovered on the Palapa Vocational School Library website, specifically in the form of SQL Injection. This vulnerability allows unauthorized access to the database, where attackers can view sensitive information and gain knowledge of login data used to access the backend of the library's website. This indicates that the library's website still has security weaknesses and is not fully protected from external threats. Therefore, to validate this finding, further testing was conducted using the penetration testing method, aimed at ensuring that the website is secure from potential exploitation.

Penetration testing was chosen because it allows for legal system exploitation to identify security gaps. Penetration testing is a recommended method to ensure system security, as it enables comprehensive testing to identify and exploit potential weaknesses within the system (Hermawan, 2021). Although the initial testing confirmed the presence of vulnerabilities, the severity of each vulnerability was not fully understood, necessitating further analysis using the Common Vulnerability Scoring System (CVSS) version 3.1. Considering that the library's website provides information accessible by students and staff, it is important for the school to implement corrective solutions to improve the website's security.

Several previous studies have shown relevant results related to this testing. One example is the research conducted by Andria and Ridho Pamungkas, in which they successfully discovered an SQL Injection vulnerability on a web server. However, in their study, further exploitation to access sensitive information in the database was not carried out (Pamungkas & Andria, 2020). Additionally, research by Rudi Hermawan explained the process of exploiting SQL Injection vulnerabilities in a web server application, although this study did not use CVSS as a tool to assess the severity of the vulnerability (Hermawan, 2021). Based on the above discussions, this study will be conducted with the title "System Security Testing Using Penetration Testing Method on the Palapa Vocational School Library Website." The aim of this study is to identify and enhance the security of the library's website, thereby minimizing the risks from unauthorized access and protecting the school's information data.

1.1 Literature Review

Information Security

Information security is a critical aspect of managing an organization's data assets. With the rapid advancement of technology, the threats to information have become increasingly complex, ranging from data theft, system destruction, to unauthorized access takeover. The goal of information security is to protect information from unwanted access, alteration, or destruction, allowing organizations to maintain operational continuity and minimize risks related to cybersecurity. The three main pillars of information security are Confidentiality, Integrity, and Availability, known as the CIA Triad.

- Confidentiality: Confidentiality ensures that only authorized individuals can access specific information. For instance, on the Palapa Vocational School Library website, user login data, including students and teachers, needs to be protected from unauthorized access.
- Integrity: The integrity aspect ensures that the information within the system is not altered or modified without authorization. On the library website, this means keeping data about book collections, borrowing history, and member data accurate and protected from unauthorized changes.
- Availability: Availability ensures that information is accessible to authorized parties whenever needed. At the Palapa Vocational School Library, it is crucial that the system is always available so users can access library information at any time without disruptions.

Good information security practices offer significant benefits, such as increased user trust, reduced financial risks, and enhanced productivity due to reliable and protected systems (Rohman & Setiawan, 2021).

Website

A website is a platform that provides information or services via the internet. Websites typically consist of several interconnected pages via hyperlinks and can contain various types of content such as text, images,

videos, or audio. In today's digital age, websites have become a primary means for educational institutions, including school libraries, to offer easy and efficient access to information.

For example, the Palapa Vocational School Library website allows students and teachers to access book information, borrowing history, and the latest news from the library without having to visit the location. Furthermore, websites also serve as effective communication and promotional tools to spread information about the library's programs and services (Adams & Walters, 2022).

Penetration Testing

Penetration testing is a method used to evaluate the security of a system or network by simulating attacks from external or internal parties. The main objective of penetration testing is to identify and exploit potential security vulnerabilities within the system. This testing is crucial for helping organizations understand existing security risks and develop better mitigation strategies.

Penetration testing can be conducted manually by security analysts or automated using specialized software. On the Palapa Vocational School Library website, penetration testing helps identify security gaps, such as SQL Injection or vulnerabilities that allow unauthorized access to the database. This testing provides clear insights into how potential attacks could affect data security and identifies steps for remediation (Jones & Harrison, 2021).

NIST SP 800-115

The National Institute of Standards and Technology (NIST) is a body that plays a role in developing security and technology standards in the United States. One of the critical documents for information security practices is NIST SP 800-115. This document provides guidelines and methodologies for conducting security testing, including penetration testing, in the form of standards and best practices that can be widely applied.

NIST SP 800-115 covers techniques to identify, evaluate, and address security vulnerabilities in web applications. This guide helps organizations outline effective and structured testing steps. In the context of the Palapa Vocational School Library website, the methodology from NIST SP 800-115 can be used as a reference to evaluate the website's security and ensure all potential vulnerabilities are identified and addressed according to standard procedures (NIST, 2020).

SQL Injection

SQL Injection is a type of attack that exploits weaknesses in SQL queries to gain unauthorized access to a database. This attack typically occurs when user input is not properly validated, allowing attackers to inject malicious SQL code. SQL Injection attacks can be highly detrimental because attackers can access or even alter sensitive information in the database, such as personal data, user login information, or financial data.

On the Palapa Vocational School Library website, SQL Injection vulnerabilities could potentially threaten important data stored in the database, including library member data or book borrowing history. Early detection of this vulnerability is crucial to protect the security of the data and prevent information leakage (Singh & Patel, 2022).

Black Box Testing

Black box testing is a testing method that assesses the functionality of a system without knowledge of its internal code or structure. The primary focus in black box testing is to ensure that the application functions correctly based on specifications and that the application's input and output align with expectations. This method does not require technical or programming knowledge from the tester, making it highly effective in identifying issues at the user interface level.

In the context of penetration testing on the Palapa Vocational School Library website, black box testing allows the tester to assess the website's security from the user's perspective, without knowing how the system is built. This technique is useful for detecting vulnerabilities that could be exploited by attackers from outside the system without access to the application's source code or structure (Robinson & Thorne, 2021).

SQLmap

SQLmap is an open-source tool widely used in penetration testing to detect and exploit SQL Injection vulnerabilities in web applications. SQLmap can automatically analyze and examine an application's database, search for SQL Injection vulnerabilities, and perform controlled exploitation. This tool comes with features that enable testing on various database types, including MySQL, PostgreSQL, and Microsoft SQL Server.

In the case of security testing on the Palapa Vocational School Library website, SQLmap can be used to detect whether SQL queries are vulnerable to attacks. Therefore, this tool helps the security team identify and assess the severity of SQL Injection vulnerabilities found, providing a basis for taking appropriate mitigation actions (Lee & Jackson, 2022).

2. Research Methods

The method applied in this research is penetration testing, based on the guidelines issued by the National Institute of Standards and Technology (NIST) under the code NIST SP 800-115. This method consists of four main stages: planning, discovery, attack, and reporting.

Fig. 1 Penetration Testing

The stages of penetration testing based on the NIST SP 800-115 guidelines are illustrated in Figure 1 and described as follows:

Planning

The planning stage is a crucial step in the penetration testing process, as it sets the foundation for the entire assessment. During this stage, researchers and the targeted organization collaborate to define and agree on the scope and objectives of the testing. Key aspects discussed include the primary goals of the penetration test, the specific areas or systems to be tested, the time frame for conducting the test, and the expected outcomes. For instance, the scope may include testing web applications, databases, or network configurations, depending on the organization's priorities. This stage is critical because it ensures that all parties have a clear understanding of the testing parameters and the rules of engagement, such as avoiding tests that could disrupt essential services. Additionally, the planning phase helps allocate necessary resources, such as tools, personnel, and timelines, to ensure the process runs smoothly and achieves the desired outcomes. Importantly, no technical testing activities are performed at this stage, as the focus is solely on preparation and strategic planning (NIST, 2020).

Discovery

The discovery phase is the information-gathering stage of penetration testing, and it is divided into two key parts: reconnaissance and vulnerability analysis. In the reconnaissance part, testers collect preliminary information about the target system, such as domain names, IP addresses, operating systems, open ports, and the services or applications running on the network. This data is typically gathered using various scanning tools and techniques, such as network mapping or service enumeration, which help outline the system's surface area that could potentially be exploited. After gathering this information, testers proceed to vulnerability analysis, where they analyze the collected data to identify security weaknesses. This step often involves cross-referencing known vulnerabilities, assessing misconfigurations, and determining outdated software versions

that could be exploited. The discovery phase is fundamental in understanding the system's potential entry points and serves as the foundation for subsequent attack simulations. Comprehensive information gathering during this stage ensures that no critical vulnerabilities are overlooked, thereby improving the overall effectiveness of the penetration test (NIST, 2020).

Attack

The attack stage is the most hands-on phase of the penetration testing process, as it involves actively attempting to exploit identified vulnerabilities to assess their impact. During this phase, testers simulate real-world attack scenarios by using the information gathered in the discovery phase to exploit weaknesses in the target system. This may include conducting SQL injection attacks, cross-site scripting (XSS), or buffer overflow exploits, depending on the vulnerabilities identified. Successful attacks provide valuable insights into how an attacker could potentially compromise the system, gain unauthorized access, or disrupt services. Conversely, if the attack fails, testers may gather additional information about the system's defenses, which could lead to further refinements in their approach. In some cases, testers may return to the discovery phase to conduct additional analysis and testing. This iterative process ensures thorough examination of the system's security posture. The attack phase is crucial for demonstrating the real-world implications of vulnerabilities and providing actionable insights for remediation (NIST, 2020).

Reporting

The reporting stage is the culmination of the penetration testing process, where all findings and insights are documented in a comprehensive report. This report typically includes detailed descriptions of the vulnerabilities discovered during the testing, the methods used to exploit them, and the potential risks they pose to the organization. Additionally, the report assigns severity levels to each vulnerability using standardized scoring systems, such as the Common Vulnerability Scoring System (CVSS). Furthermore, the report provides actionable recommendations for mitigating these vulnerabilities, helping the organization prioritize remediation efforts based on risk levels. The reporting stage not only ensures accountability but also serves as a valuable resource for stakeholders, enabling them to implement targeted improvements to their security posture. A well-structured report facilitates communication between technical teams and management, bridging the gap between technical findings and strategic decision-making. This stage underscores the importance of penetration testing as an essential tool for enhancing organizational cybersecurity (NIST, 2020).

3. Result and Discussion

Planning

In the planning phase, the researcher defines and prepares for the penetration testing process. This phase must adhere to the methodology outlined in NIST SP 800-115. Therefore, comprehensive planning and preparation are conducted as follows:

- Scope of Work

Interviews were conducted with Guntur, S.Kom., an Information and Communication Technology (ICT) staff member specializing in information security, and the staff of SMK Palapa Library to define the scope of testing for this research. The agreements reached during this phase include:

Confirmation of the approach and explanation of the penetration testing methodology based on NIST SP 800-115, which will be applied to identify vulnerabilities in the SMK Palapa Library website.

- Approval to use the Black Box Testing technique for conducting the penetration testing.
- Focused testing on the login form menu, where SQL Injection vulnerabilities have been identified.
- Agreement on the tools to be used during penetration testing.
- Submission of the final report to the management of SMK Palapa Library.

- Analysis of Testing Tool Requirements

This study identifies the tools needed for conducting penetration testing, which consist of hardware, software, and specific tools. One essential tool selected for this process is OWASP ZAP (Zed Attack Proxy), a widely used open-source tool for identifying vulnerabilities in web applications, including SQL Injection and other potential security flaws.

Discovery Phase
In the discovery phase, OWASP ZAP was used to identify potential vulnerabilities by gathering information and analyzing the target system.

Information Gathering:

- Target: The login form of the SMK Palapa Library website.
- ZAP was configured to perform a spider crawl, identifying directories, endpoints, and hidden links within the website.
- Results: ZAP successfully mapped out the structure of the website, revealing hidden directories and form fields that could be exploited.

Vulnerability Scanning:

- Using ZAP's active scanning feature, potential security weaknesses were identified.
- Results:
  - Sensitive Information Disclosure: ZAP flagged a directory containing configuration files that exposed sensitive information, such as API keys and environment variables.
  - SQL Injection: ZAP detected improper input sanitization on the login form, indicating the potential for SQL Injection attacks.

Attack Phase
In the attack phase, the vulnerabilities identified during discovery were tested to confirm their exploitability.

Sensitive Information Disclosure:

- Exploit: The exposed configuration directory allowed unauthorized access to sensitive data, including a file that contained partial database credentials.
- Impact: This vulnerability could enable attackers to escalate their privileges and access the back-end system.

SQL Injection:

- Exploit: ZAP was used to simulate malicious payloads on the login form. SQL payloads such as admin' OR '1'='1 successfully bypassed the authentication mechanism, granting access to the administrative dashboard.
- Impact: Exploitation of this vulnerability exposed sensitive user data, including usernames, passwords (in hashed format), and borrowing records.

Reporting
The reporting phase is the final stage based on the NIST SP 800-115 standard. In the previous stages, the researcher collected vulnerability findings and simulated attacks on the identified vulnerabilities. The report has been created as a table and saved in Word format. You can download it using the following link:

Table 1. Reporting Results

Vulnerability	Severity (CVSS v3.1)	Description	Impact	Recommendations
SQL Injection	Critical (9.8/10)	Improper input sanitization on login form.	Exposes sensitive data like usernames and passwords; potential	1. Implement input validation to sanitize user inputs. 2. Use parameterized

			unauthorized access to admin dashboard.	queries or prepared statements in database operations. 3. Conduct regular penetration testing.
Sensitive Information Disclosure	Medium (5.0/10)	Exposed directories containing configuration files with sensitive data.	Potential unauthorized access to server configurations and API keys.	1. Restrict access to sensitive directories using proper server-side configurations. 2. Encrypt sensitive files and remove unused or temporary files from the server.

4. Conclusions

After receiving a report from a bug hunter regarding vulnerabilities in the SMK Palapa Library website, the researchers confirmed the findings through testing using the penetration testing method, based on the NIST SP 800-115 standard. The testing was conducted in four stages: planning, discovery, attack, and reporting, successfully identifying two vulnerabilities in the SMK Palapa Library website: sensitive information disclosure and SQL Injection.

During the testing, a sensitive information disclosure vulnerability was discovered, allowing unauthorized access to view the directory of the login form leading to the back-end page. Additionally, an SQL Injection vulnerability was identified, capable of exposing sensitive information, such as usernames and passwords, which could potentially be misused by unauthorized parties. Risk assessment using CVSS version 3.1 classified the SQL Injection vulnerability as critical in severity, while the sensitive information disclosure vulnerability was rated as medium. As a follow-up, the researchers provided appropriate remediation solutions for both vulnerabilities to enhance the security of the SMK Palapa Library website.

5. References

Andria, & Pamungkas, R. (2020). Penetration testing database menggunakan metode SQL Injection via SQLmap di Termux. IJAI (Indonesian Journal of Applied Informatics), 5(1), 1–10.

Dhaifullah, I. R., Muttanifudin, M., Salsabila, A. A., & Yakin, M. A. (2022). Survei teknik pengujian software. Journal Automation Computer Information System, 2(1), 1–8.

Endra, R. Y., Aprilinda, Y., Dharmawan, Y. Y., & Ramadhan, W. (2021). Analisis perbandingan bahasa pemrograman PHP Laravel dengan PHP Native pada pengembangan website. Jurnal Manajemen Sistem Informasi dan Teknologi, 11(1), 1–8. https://doi.org/10.36448/expert.v11i1.2012

Hermawan, R. (2021). Teknik uji penetrasi web server menggunakan SQL Injection dengan SQLmap di Kali Linux. STRING (Satuan Tulisan Riset dan Inovasi Teknologi), 6(2), 1–7.

Jaelani, W. L., Yanto, & Khoirunnisa, F. (2023). Penetration testing website dengan metode black box testing untuk meningkatkan keamanan website pada instansi (Redacted). Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika, 5(1), 1–8.

Lawa, H. W., Kwuta, Y. D. D. Y., & Sala, E. E. (2023). Sistem informasi pengelolaan bantuan dana desa Hangalande berbasis web. Jurnal Sistem Informasi dan Teknik Komputer, 8(1), 1–7.

Maherza, S. A., Hananto, B., & Pradnyana, I. W. W. (2023). Penetration testing terhadap website sekolah menengah atas ABC dengan metode NIST SP 800-115. Jurnal Informatik, 19(1), 1–17.

Novrian, R., Sovianti, R., & Mubarok, M. H. (2021). Pendampingan dan sosialisasi manajemen komunikasi penanganan kasus kekerasan seksual pada anak di Dinas P3A dan 18 Kelurahan Kota Bekasi. Jurnal Pengabdian Masyarakat Multidisiplin, 2(2), 1–9.

Putranto, D. P., Jayanta, & Hananto, B. (2022). Analisis keamanan website Leads UPNVJ terhadap serangan SQL Injection & sniffing attack. JURNAL INFORMATIK, 18(3), 1–9.

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi keamanan website lembaga X melalui penetration testing menggunakan framework ISSAF. Jurnal Ilmiah Merpati, 8(2), 1–12.

Sofyan, H., Sugiarto, M., & Akbar, B. M. (2023). Implementation of penetration testing on websites to improve security of information assets UPN 'Veteran' Yogyakarta. Jurnal Informatika dan Teknologi Informasi, 20(2), 1–10. https://doi.org/10.31515/telematika.v20i2.7757

Triandi, B. (2019). Keamanan informasi secara aksiologi dalam menghadapi era revolusi industri 4.0. Jurnal Riset Komputer (JURIKOM), 6(5), 1–7. Available at: http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom|Page477

Utama, I. M. P., Putri, K. R., Wirayuda, A. A. E., & Tyora, V. A. (2022). Analisis perbandingan kinerja tool website directory brute force dengan target website DVWA. Jurnal Informatik, 18(3), 1–8. Available at: https://www.kali.org/get-kali/#kali-platforms

Wardhana, M. A. W., Pratama, K. D. P., & Muryani, S. (2022). Aplikasi informasi pemeliharaan alat produksi pada PT. Teguh Karya Perima. Jurnal Infortech, 4(2), 1–8. Available at: http://ejournal.bsi.ac.id/ejurnal/index.php/infortech148

Yusnanto, T., Muin, M. A., & Wahyudiono, S. (2022). Analisa infrastruktur jaringan wireless dan local area network (WLAN) menggunakan Wireshark serta metode penetration testing Kali Linux. Journal on Education, 4(4), 1–7.

Zen, B. P., Gultom, R. A. G., & Reksoprodjo, A. H. S. (2020). Analisis security assessment menggunakan metode penetration testing dalam menjaga kapabilitas keamanan teknologi informasi pertahanan negara. Jurnal Teknologi Penginderaan, 2(1), 1–18.