Analysis of Website Vulnerabilities Utilizing OWASP on the Enterpreneurship Locker System

Andre Kurniawan Pamudji[1], Florentinus Budi Setiawan [3]
Engginering Profession Soegijapranata Catholic University Semarang
Jl. Pawiyatan Luhur no IV/1, Semarang, 50234, Indonesia
[1]andre.kurniawan@unika.ac.id, [2]f.budi.s@unika.ac.id

Abstract— The government's restrictions on activities during the Covid-19 pandemic resulted in the closure of numerous activities. This has resulted in the closure of numerous businesses, particularly small and medium-sized enterprises, as a result of a lack of customers. Therefore, a new invention was developed in the field of Entrepreneurial Lockers that enables transactions to be conducted without the need for face-to-face interaction and without the use of cash. This innovation entails the development of a website that serves as a digital ordering and payment system. In order to ensure that users feel secure while using the website, it is imperative to assess the website's data security to prevent the occurrence of any unintended events. The OWASP method is employed in this investigation to assess the security of the IoT-based entrepreneurial storage system in order to identify critical security vulnerabilities. The findings indicate that the system has satisfied numerous security standards; however, it necessitates improvement in the areas of access control, framework updates, and logging. This investigation offers suggestions for enhancing the security of data in IoT-based systems.

Keywords— OWASP, Web Security, Enterpreneur Locker, payment system

I. INTRODUCTION

The Covid-19 pandemic, which began in Indonesia in March 2020, has resulted in the discontinuation of different activities due to mandates for remote engagement to decrease virus transmission within the community. Several steps have been implemented to minimize the rate of viral transmission, including the imposition of restrictions on community activities (PPKM), which began on July 3 in Java-Bali. [1]. In September 2021, the spread of the Covid-19 viral pandemic began to slow, and some activities, including those in school, resumed. The government has begun to promote for the implementation of restricted face-to-face learning in the educational sector, allowing students to participate in offline learning activities at their individual institutions. Although face-to-face learning activities are still possible, because to the large number of Covid-19 instances, school canteen operations must be halted to avoid overcrowding, advising students to bring their own supplies. As a result, it is critical to have cutting-edge solutions that can assist business players in maintaining operations despite the drop caused by the pandemic. [2].

This project creates a prototype product modeled around an entrepreneurial locker with automated servicing. This project aims to revitalize canteen entrepreneurship in educational institutions. This paper describes a locker that combines the advancements of the Internet of Things (IoT) with a cashless payment mechanism based on QRIS. The creation of an entrepreneurial locker allows school canteen sellers to keep their food in a specific locker compartment. Buyers can then access the food through the system and complete cashless transactions via QRIS, which causes the locker door to open immediately upon successful payment. The strategy used will decrease the physical interaction between parties. [3], [4], [5].

The Internet of Things (IoT) is a concept that uses the internet to simplify everyday chores, such as managing gadgets

in our environment. The Internet of Things (IoT) has been acknowledged since 2009 and has had a substantial impact on various areas, including government, industry, education, and health [6]. The use of IoT in the design of entrepreneurial lockers acts as a method to restrict door opening, allowing automated access following a successful transaction.

QRIS is a cashless payment system that utilizes QR codes to expedite the payment process. It was developed collaboratively by the payment system industry and Bank Indonesia [7], [8]. QRIS is a well-known payment system in Indonesia, and many users use it to streamline the transaction process. QRIS is now a legitimate payment alternative, accepting transactions via several E-Wallets such as Go-Pay, OVO, Dana, LinkAja, and others. This will improve consumer involvement and interest in using QRIS services. Implementing QRIS helps to reduce physical interaction by enabling cashless transactions.

This innovation is intended to alleviate the operational issues that small and medium-sized organizations, particularly those in the education sector, encounter as a result of physical activity limits. [9]. This technology automates the ordering and payment processes, eliminating physical interactions and enhancing operational efficiency.

While digital technology offers many advantages, it also introduces some risks, particularly regarding the security of user data and the potential for cyberattacks. When designing a digital payment system, it is crucial to thoroughly assess the system to ensure it operates smoothly and remains secure for users. One effective way to evaluate a system's security is by using the Open Web Application Security Project (OWASP) framework. This method helps developers identify and address common security vulnerabilities that could jeopardize the integrity of a website. OWASP provides a "Top Ten" list of critical security risks, highlighting the most prevalent threats to web applications. By using these guidelines, developers can pinpoint weaknesses in their systems early, reduce the likelihood of unexpected issues, and take proactive steps to safeguard against potential hacker attacks.. [11][12].

This study studies and evaluates the entrepreneurial locker system using the OWASP approach to determine its security level.

II. METHODOLOGY

This research begins by determining the test target, namely the website of the entrepreneurial job booking and payment system using the OWASP method.

The research method can be seen in Figure 1. related to the research flow.

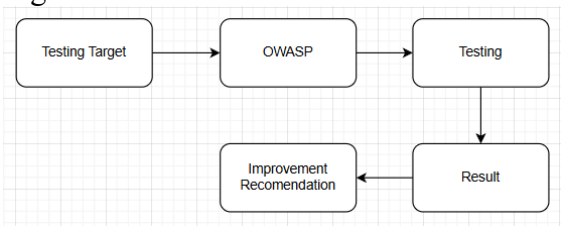

Figure 1. Research Flow

General information about the testing target can be found in Table 1. Website information.

Table 1. Infrastructure Information

Informasi Infrastruktur	
cPanel Version	124.0 build 10
Apache Version	2.4.59
Database Version	10.5.22-MariaDB-cll-lve
Arsitektur	x86_64
Operating System	linux

The OWASP methodology used in this study includes

1. Injection is a method used to check the system for vulnerabilities by injecting code, such as SQL injection, command injection, or cross-site scripting (XSS).
2. Broken Authentication is a method of ensuring strong authentication, such as passwords that can be easily forgotten, and shortening

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v11i2.13103

session times to allow access to some areas for those without access rights.

3. Sensitive Data Exposure Exposing is the process of ensuring sensitive data in a system, such as credit card, password, and pin, is safe and difficult to identify, reducing the risk of data breaches.
4. XML External Entities. Using XML entities, this method is used to conduct checks on the website's responsiveness to user queries.
5. Broken Access Control is a method to check for improper access control, allowing unauthorized users to access data that should not be accessible.
6. Security Misconfiguration is a method for analyzing and updating network configurations to ensure they are always up-to-date with changing requirements.
7. Cross-Site Scripting is used to prevent malicious scripts from being accessed by other users, which can lead to data breaches, session hijacking, and other issues.
8. Insecure deserialization is a method for checking data integrity, which can lead to incorrect code execution, service failure, and other issues.
9. Using a component with known vulnerabilities. This method is an analysis of the components of a person's life or rent that can be used to create a rent-based application..
10. Insufficient Logging and Monitoring. This insufficient method is used to analyze the log data that is used on the system to ensure that each activity can be tracked, hence assisting the decision-making process when a security issue occurs. [13], [14], [15].

III. RESULT AND DISCUSSION

The following are the results of the OWASP-based analysis performed on a enterpreneurship locker website.

.

1. Injection, during the analysis of the website's security features, it was observed that the login process employs the htmlspecialchars function, a PHP script designed to convert special characters in user inputs into their corresponding HTML entities. This implementation aims to detect and mitigate potential Cross-Site Scripting (XSS) attacks, which occur when malicious scripts, such as HTML or JavaScript tags, are injected into a web application. By converting special characters such as "<" and ">" into their safe encoded versions (< and >), this function ensures that these characters are viewed as simple text rather than executable code. This helps protect the login process from potential cross-site scripting (XSS) attacks, effectively bolstering the security of the system.

Figure 2. Injection Analysis

2. Broken Authentication: When a website allows multiple failed login attempts—typically more than three—the system triggers a security feature known as a "lockout mechanism." This lockout temporarily blocks the

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v11i2.13103

user from accessing their account, providing protection against brute force attacks, where hackers attempt to guess usernames and passwords by trying different combinations repeatedly. While this mechanism helps prevent unauthorized access, it can sometimes create usability issues for legitimate users, especially if they forget their login details or make multiple incorrect attempts in a short period.

Figure 3. Broken Authentication Analysis

3. The code used in the query, as demonstrated in Figure 2, is carefully designed to reduce the risk of exposing sensitive data. The query is specifically structured to pull only the data that is necessary for the task at hand. This approach ensures that no extra, irrelevant information is included in the process, thereby minimizing the chance of unintentionally revealing sensitive details like personal identification, financial information, or internal system secrets that aren't required for the operation. By narrowing the scope of the data being retrieved, the system helps ensure that only authorized and relevant information is accessible. This strategy significantly lowers the risk of unauthorized access to sensitive data and reduces the potential vulnerabilities that could be exploited by attackers. In this way, the system's design strengthens security by minimizing the attack surface and limiting the exposure of critical data.
4. XML External Entities (XXE): In the security analysis of the website, it was found that the system does not implement or utilize XML functionality or data processing mechanisms, which significantly reduces the risk of XML External Entity (XXE) attacks. XXE vulnerabilities occur when an application processes untrusted XML input containing references to external entities, which can be exploited by attackers to execute malicious actions, such as accessing internal files, performing denial-of-service (DoS) attacks, or even executing arbitrary code on the server.
5. Broken Access Control, in the case of Broken Access Control, each admin pages is followed by the process of checking the user's session; if a page does not have a suitable session, the user will be directed to the login page to complete the login process.

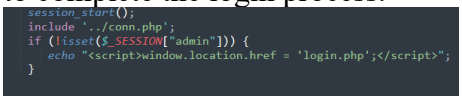

Figure 4. Broken Access Control Analysis

6. Security Misconfiguration, the website in issue has already implemented the HTTPS security protocol, but it has not yet implemented an updated framework with a built-in security system. Websites that are being built use a process that

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v11i2.13103

begins from scratch.

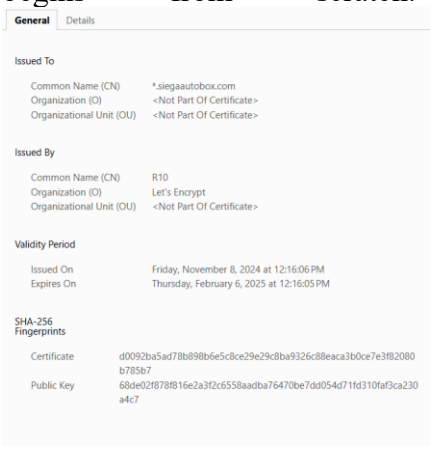

Figure 5. Security Misconfiguration Analysis

7. Cross-Site Scripting
   The website has used the htmlspecialchars function to validate user input, allowing it to prevent malicious script injection. However, this method has limitations in terms of addressing all types of XSS, such as DOM-based attacks. As a result, more comprehensive input filter implementation is required, such as using a contemporary library (for example, OWASP ESAPI).
   Sensitive data exposure: The results of the analysis show that the SQL query used is only suitable for retrieving the data required. However, sensitive data, such as kata sandi, does not use a strong hashing algorithm (such as bcrypt), therefore there is a risk if the base data.

```php
include '../conn.php';
$uploadOk = 1;
$id = $_POST['id'];
$nama = $_POST['nama'];
$harga = $_POST['harga'];
$deskripsi = $_POST['deskripsi'];
$penjual = $_POST['penjual'];

// Sanitize user input to prevent XSS
$nama = htmlspecialchars($nama, ENT_QUOTES);
$harga = htmlspecialchars($harga, ENT_QUOTES);
$deskripsi = htmlspecialchars($deskripsi, ENT_QUOTES);
$penjual = htmlspecialchars($penjual, ENT_QUOTES);
```

Figure 6. Cross Site Scripting Analysis

8. Insecure Deserialization
   The chosen website also lacks data serialization capabilities such as JSON, making it vulnerable to the effects of insecure deserialization.
9. Using Component with Known Vulnerabilities
   The website utilizes several external libraries via CDN (Content Delivery Network), including Bootstrap, jQuery, and Font Awesome. Each library is a unique component of the network that can have previously unknown or improved security features. As a result, an update must be performed on the existing libraries.

Figure 7. Using Component with Known Vulnerabilities Analysis

10. Insufficient Logging and Monitoring
    On the system database that is being analyzed, there is a significant issue with the logging system, which currently lacks the capability to capture and track user activities effectively. This absence of proper logging mechanisms creates a gap in the system's ability to monitor and record critical actions performed by users, making it difficult to detect potential security incidents, unauthorized access, or misuse of the system.

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v11i2.13103

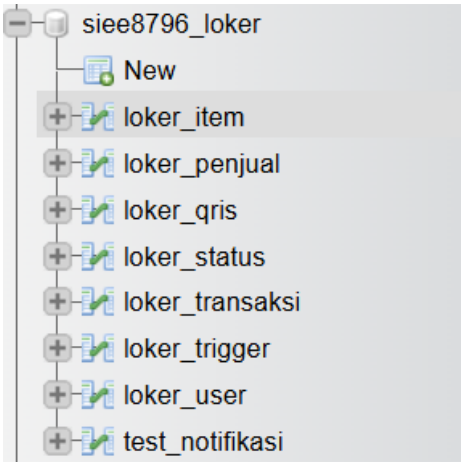

Figure 8. Logging Analysis.

IV. CONCLUSION

Based on the results of the audit conducted on the Enterpreneurship Locker website using the OWASP method, it is possible to conclude that the website that was built has included some system security measures, but it is not yet ideal in terms of security. There is a need for system development to ensure that the system being built is safe to use by users, such as logging, updating the framework and library to the latest version.

REFERENCES

[1] Kominfo, "Mulai 3 Juli, Pemerintah Berlakukan PPKM Darurat di Jawa-Bali." Accessed: Dec. 28, 2022. [Online].

[2] Hidayatullah Muttaqin, "Pentingnya Inovasi di Tengah Langkah Berat Perekonomian Indonesia pada Masa Pandemi Covid-19." Accessed: Dec. 28, 2022. [Online].

[3] Pamungkas Ashadi, "Meriahkan Hardiknas, Nusaputera Semarang Launching Loker Siega Autobox Digital," *Suara Merdeka*, 2023. Accessed: May 30, 2024. [Online].

[4] Yulius Bisma Cahyaprawira, Andre Kurniawan Pamudji, Tecla Brenda Chandrawati, and Erdhi Widyarto Nugroho, "Internet of Things-Based Entrepreneurship Lockers," *Journal Business and Technology*, vol. 2, no. 3, 2022, Accessed: Apr. 27, 2024. [Online].

[5] F. H. P. B. H. A. D. W. Victorio Almers Chrisetya Putra, "Financial Technology with QRIS Payment System for Entrepreneurship Locker," *Sisforma*, vol. 10, no. 1, 2023.

[6] Abbas Shah Syed, Daniel Sierra-Sosa, Anup Kumar, and Adel Elmaghraby, "IoT in Smart Cities: A Survey of Technologies, Practices and Challenges," *Smart Cities*, Mar. 2021, Accessed: Apr. 30, 2023. [Online].

[7] Denny Tenggino and Tuga Mauritsius, "Evaluation of Factors Affecting Intention To Use QRIS Payment Transaction," *ICIC Express Letters*, vol. 16, no. 4, pp. 343–349, Apr. 2022, Accessed: Dec. 28, 2022. [Online].

[8] Bank Indonesia, "QRIS," *Bank Indonesia*, 2024.

[9] Stephani Inggrit Inggrit Swastini Dewi, Andre Kurniawan Pamudji, and Agustina Alam Anggitasari, "Business Model Canvas for SIEGA Autobox Automated Locker," *SISFORMAA*, vol. 11, no. 1, 2024.

[10] Muhammad Idris, Iwan Syarif, and Idris Winarno, "Web Application Security Education Platform Based on OWASP API Security Project," *International Journal of Engineering Technology*, vol. 10, no. 2, 2022.

[11] Matthew Bach-Nutman, "Understanding The Top 10 OWASP Vulnerabilities," *ArXiv*, 2020.

[12] Dewi Aryanti, Nurholis, and Joy Nashar Utamajaya, "Analisis Kerentanan Keamanan Website Menggunakan Metode Owasp (Open Web Application Security Project) Pada Dinas Tenaga Kerja," *Syntax Fusion*, vol. 1, no. 3, 2021.

[13] Muhammad Idris, Iwan Syarif, and Idris Winarno, "Development of Vulnerable Web Application Based on OWASP API Security Risks," in *2021 International Electronics Symposium (IES)*, 2021.

[14] K. A. Sedek, N. Osman, M. N. Osman, and Hj. K. Jusoff, "Developing a Secure Web Application Using OWASP Guidelines," *Computer and Information Science*, vol. 2, no. 4, Oct. 2009, doi: 10.5539/cis.v2n4p137.

[15] OWASP Foundation, "OWASP Top Ten Web Application Security Risks 2021," 2021.