CHAPTER I
INTRODUCTION

1.1. Background

The rapid advancement of information technology has encouraged many organizations, both governmental and private, to utilize web-based applications as the primary platform for delivering services. Websites are no longer used solely to provide information, but also to facilitate transactions, communication, and the management of sensitive data. However, as the use of websites continues to increase, cybersecurity threats have also become more sophisticated and complex. Attacks targeting web applications, such as Injection, Cross Site Scripting (XSS), Broken Authentication, and various other exploits, have become critical issues that may result in financial losses, data breaches, and reduced user trust.

Indonesia continues to face significant challenges in cybersecurity. The National Cyber and Crypto Agency (BSSN) reported 403.9 million anomalous attack traffic events in 2023, including 4 million Advanced Persistent Threat (APT) activities, more than 1 million ransomware attacks, and 189 web defacement incidents. In addition, 1.67 million data records were exposed on the darknet, while 2,860 security vulnerabilities were identified across 586 national electronic systems [1]. According to the National Cyber Security Index (NCSI) 2022, Indonesia scored only 38.96 points and ranked 83rd out of 160 countries, placing it as the third lowest-ranked country among the G20 members [2].

Although Indonesia's NCSI score improved to 63.64 points in 2023, placing it fifth in Southeast Asia, its performance still lagged behind Malaysia, which scored 79.22 points, and Singapore, with 71.43 points [3]. Meanwhile, the global trend of attacks targeting web applications has shown a significant increase. The State of Application Security Report 2025 recorded more than 7.7 billion cyberattacks throughout 2024, averaging 5.5 million attacks per website. API attacks increased by as much as 873%, while DDoS attacks reached 2.46 billion incidents, with Injection and API vulnerabilities remaining the most frequently exploited threats according to the OWASP Top 10 list [4].

Therefore, ensuring the security of web applications through security testing has become an essential requirement. One of the most widely adopted approaches is

the use of vulnerability scanning tools to identify potential security weaknesses before they can be exploited by malicious actors. Various tools are currently available for this purpose, two of the most widely used being OWASP ZAP (Zed Attack Proxy) and Nessus. Both are well-known vulnerability scanners capable of detecting system weaknesses and are commonly used by penetration testers during penetration testing activities.

OWASP ZAP (Zed Attack Proxy) is an open-source penetration testing tool specifically designed to assess web application vulnerabilities. It can identify security weaknesses such as Injection, Cross-Site Scripting (XSS), and security misconfigurations. Using this tool, developers can discover potential vulnerabilities within a website and implement appropriate mitigation measures before they are exploited by attackers [5]. Meanwhile, Nessus is a vulnerability assessment tool equipped with a wide range of vulnerability detection capabilities. It enables users to identify various types of security weaknesses, including vulnerabilities affecting websites, networks, and operating systems [6].

In the context of this study, testing with these two tools should be conducted in a controlled environment to avoid causing adverse effects on production systems. Therefore, vulnerable web applications, or web application labs intentionally designed with security flaws for educational and testing purposes, are used. Several applications widely adopted by academics and information security practitioners include bWAPP, Metasploitable 3, and Zero Bank. These applications provide various attack scenarios that closely resemble real-world conditions, allowing researchers to evaluate the effectiveness of vulnerability scanning tools in detecting security weaknesses. However, this study also aims to examine the scanning results obtained from a real-world website operating in its current environment. Therefore, a limited assessment will also be conducted on Website X, which is one of the internal websites of an educational institution.

Several previous studies have identified aspects that require further development, particularly regarding the vulnerability scanning tools being compared. As web application vulnerabilities continue to evolve, vulnerability scanners are also continuously improved through newer versions. In addition, previous comparison results based only on scanning duration and validation of detected vulnerabilities are not sufficiently robust due to the lack of systematic and detailed quantitative analysis.

The absence of comprehensive quantitative metrics, such as accuracy, precision, recall, and F1-score, limits an objective evaluation of the performance of each vulnerability scanner. Therefore, this study aims to address these research gaps.

Based on the background described above, this study conducts a comparative analysis of OWASP ZAP and Nessus in detecting vulnerabilities within web applications. The comparison includes both quantitative and qualitative analyses using three vulnerable web application labs, namely bWAPP, Metasploitable 3, and Zero Bank. In addition, a qualitative comparison is conducted on Website X. The findings of this study are expected to provide a comprehensive understanding of the capabilities, coverage, and effectiveness of each tool based on measurable quantitative metrics, while also serving as a reference for developers, system administrators, and researchers in selecting the most appropriate tool for web application security testing.

1.2. Research Questions

Based on the background of the problem described above, the research problems are identified as follows:

1. How effective is OWASP ZAP in detecting vulnerabilities in vulnerable web application labs (bWAPP, Metasploitable 3, and Zero Bank) and Website X?
2. How effective is Nessus in detecting vulnerabilities in vulnerable web application labs (bWAPP, Metasploitable 3, and Zero Bank) and Website X?
3. What are the differences in the vulnerability detection results obtained from OWASP ZAP and Nessus?
4. To what extent are these two tools effective in detecting vulnerabilities in web applications?

1.3. Research Objectives

The research objectives represent the goals to be achieved through this study. Therefore, the objectives of this study are as follows:

1. To analyze the effectiveness of OWASP ZAP in detecting vulnerabilities in vulnerable web application labs (bWAPP, Metasploitable 3, and Zero Bank) and Website X.

2. To analyze the effectiveness of Nessus in detecting vulnerabilities in vulnerable web application labs (bWAPP, Metasploitable 3, and Zero Bank) and Website X.
3. To compare the vulnerability detection results obtained from OWASP ZAP and Nessus.
4. To evaluate the effectiveness of both tools in detecting vulnerabilities in web applications.

1.4. Research Benefits

The benefits of this study are as follows:

1. To expand knowledge and enrich the existing literature in the field of web application security, particularly regarding the effectiveness of vulnerability scanning tools.
2. To provide insights for web application developers in understanding potential vulnerabilities that may arise, while also offering recommendations on suitable vulnerability scanning tools for security testing.
3. To serve as a reference for institutions and organizations in selecting the most appropriate vulnerability scanning tool, either OWASP ZAP or Nessus, based on their security priorities, whether at the web application or network infrastructure level.
4. To support researchers and students by providing a valuable reference and learning resource on the comparative effectiveness of vulnerability scanning tools in the context of web application security.

1.5. Scope of Research

To maintain the focus of this study and prevent the scope from becoming too broad, the following research limitations are defined:

1. The vulnerability analysis is limited to vulnerabilities ranging from the highest to the lowest severity levels, excluding informational vulnerabilities.
2. Vulnerability validation on Website X is conducted based on the scanning results generated by both vulnerability scanning tools.