CHAPTER I
INTRODUCTION

1.1. Background

The development of information and communication technology has had a significant impact on various aspects of human life. The presence of the internet is now not only used to search for information and communicate, but its use has also expanded across many fields. The growing number of internet users each year has driven major changes in patterns of interaction, ways of working, learning systems, and economic activities that have shifted to the digital realm.

One of the sectors that has grown rapidly due to digitalization is trade, where many businesses have shifted to electronic platforms (e-commerce). E-commerce is a platform that facilitates buying and selling activities of goods or services through electronic systems [1]. Based on data from the Central Statistics Agency (BPS), the number of e-commerce businesses in 2022 reached 2,995,986 units, then increased to 3,816,750 units in 2023, representing a growth of approximately 27.40% in just one year [2]. The presence of e-commerce has made it easier for people to conduct transactions. Purchases of goods and services can now be made anytime and from anywhere via computer or smartphone, further accelerated by increasingly diverse digital payment methods and various supporting platforms.

As e-commerce grows rapidly, cybersecurity challenges have become a serious threat that can harm both users and service providers. The rise of online transactions, supported by easy access and digital payment methods, has also opened opportunities for cybercrime such as hacking, data theft, and fraud. These threats can undermine user confidence in the future of e-commerce platforms. According to a report by the National Cyber and Crypto Agency (BSSN), the number of cyberattacks in Indonesia showed a significant upward trend from 2020 to 2024, with recorded traffic of 316.17 million in 2020, declining to 266.74 million in 2021, rising to 370.02 million in 2022, surging drastically to 603.28 million in 2023, and increasing by 1.04% from the previous year to reach 610.63 million attacks in 2024 [3]. In 2020, Tokopedia made headlines after 91 million user account records and 7 million merchant records were leaked and traded on the dark web for approximately IDR 70 million, highlighting the weak security of digital platforms [4]. Such vulnerabilities are often caused by security gaps in platforms, such as authentication failures, malicious code injection, or insecure

system configurations. The e-commerce industry faces four main security issues: transactional security, data privacy, system security, and cybercrime such as fraud or hacking attacks [5].

Given the various security threats occurring in the cyber world, strategic measures are needed to ensure the security of e-commerce platforms. One important effort is conducting security testing to identify, evaluate, and minimize vulnerabilities that could be exploited by irresponsible parties. According to [6], security testing plays a crucial role in addressing the high level of cyber threats that could potentially cause service disruptions or data breaches. Beyond detecting technical weaknesses, such testing also helps service providers improve system reliability and maintain user trust. In line with this, penetration testing focuses on identifying exploitable gaps so that organizations can immediately carry out mitigation and strengthen their defenses before they are actually exploited by attackers [7].

PT. XYZ is a company that manufactures mattresses and is currently expanding its operations into the digital realm by launching its first e-commerce website. Although still relatively new, the site has successfully attracted considerable user traffic, with 18,788 visitors recorded in the period from July to September 2025. However, no penetration testing has ever been conducted, meaning the site potentially harbors vulnerabilities, particularly in the implementation of critical features such as the checkout process, payment gateway integration, and customer data management. Therefore, structured security testing is necessary to prevent operational disruptions and financial losses in the future.

In practice, there are several standards and frameworks commonly used to carry out security testing. The Penetration Testing Execution Standard (PTES) is one of the widely used penetration testing method standards. PTES provides structured guidance for conducting penetration tests, covering several stages from pre-engagement, information gathering, vulnerability analysis, exploitation, post-exploitation, to reporting. With this framework, the security testing process can be carried out in a more directed, measurable, and consistent manner [8].

To complement the use of PTES, NIST SP 800-115 is also available, issued by the National Institute of Standards and Technology. This document provides technical guidance on information security testing methods covering planning, execution, and

reporting of security tests. By referring to NIST SP 800-115, the implementation of PTES can follow international standards, making the test results more accountable [9].

Meanwhile, OWASP Top 10 is a list of the ten most critical vulnerabilities commonly found in web applications, including e-commerce platforms. This list is compiled by the Open Web Application Security Project (OWASP) based on the frequency and severity of gaps found in the real world. By referring to OWASP Top 10, security testing can be focused on the types of vulnerabilities most frequently exploited by attackers, helping the penetration testing team plan inspection priorities, improve testing efficiency, and ensure that the most potentially harmful risks can be identified and addressed [10].

Based on the problems described, and given the absence of any prior security testing, this research is focused on identifying security gaps in PT. XYZ's e-commerce website and providing appropriate mitigation recommendations to minimize the potential for exploitation. The testing process will be carried out through penetration testing using the PTES approach, while vulnerability classification refers to OWASP Top 10 and the testing stages are guided by the NIST SP 800-115 standard.

1.2. Problem Formulation

Based on the background described above, the research problems can be formulated as follows:

1. How can potential vulnerabilities in PT. XYZ's e-commerce website be identified by referring to the OWASP Top 10 categories?
2. How are the stages of the Penetration Testing Execution Standard (PTES) method applied in the security testing of PT. XYZ's e-commerce website based on OWASP Top 10 and the NIST SP 800-115 guidelines?

1.3. Research Objectives

Based on the problem formulation above, the objectives to be achieved in this research are as follows:

1. To identify potential security vulnerabilities in PT. XYZ's e-commerce website by referring to the OWASP Top 10 categories.

2. To implement the stages of the Penetration Testing Execution Standard (PTES) method in the security testing of PT. XYZ's e-commerce website guided by OWASP Top 10 and NIST SP 800-115.

1.4. Research Benefits

Based on the results of the research conducted, the benefits expected to be obtained from this research are as follows:

1. To provide a clear picture of the security vulnerabilities present in PT. XYZ's e-commerce website along with technical remediation recommendations as a basis for mitigation.
2. To serve as a reference for the application of the PTES method guided by NIST SP 800-115 and OWASP Top 10 in e-commerce website security testing.
3. To expand knowledge and practical insight in the field of cybersecurity, particularly penetration testing on web applications.

1.5. Research Limitations

In this research, there are several limitations that need to be considered, namely:

1. The research is focused solely on security testing of PT. XYZ's e-commerce website.
2. Security testing is conducted using the PTES method and guided by OWASP Top 10 and NIST SP 800-115; therefore, anything outside these standards is not the focus of this research.
3. Integration with the third-party payment gateway (Midtrans) is tested only in terms of its implementation on the e-commerce website side, and does not include the internal systems of the payment gateway itself.
4. This research is limited to the process of identifying vulnerabilities and discussing technical remediation recommendations in accordance with OWASP vulnerabilities.