CHAPTER I
INTRODUCTION

1.1 Background

The rapid evolution of information technology has fundamentally reshaped contemporary corporate infrastructure, particularly through the implementation of Enterprise Resource Planning (ERP). This unified software platform serves to coordinate and optimize vital organizational operations, including financial accounting, supply chain logistics, manufacturing, human resources, and customer relationship management [1]. By centralizing operational processes and data into a single platform, ERP aims to improve efficiency, data consistency, and the effectiveness of corporate decision-making.

However, the increasing reliance on web-based systems is accompanied by greater cybersecurity risks. According to a report by The Straits Times (2024), more than 40 government agencies in Indonesia were affected by a cyberattack targeting the national data center, causing disruptions to various critical public services, including immigration services and airport operations. These attacks utilized ransomware that paralyzed systems and demanded large ransoms, indicating that the national digital infrastructure still has significant security vulnerabilities [2]. These findings support a report by the National Cyber and Cryptography Agency (BSSN, 2025), which revealed that cyber threats in 2025 are becoming increasingly serious, particularly for Indonesia's financial sector. Digital attacks are no longer merely about stealing data; they now directly target financial losses and business reputation. From ransomware that paralyzes public service operations to AI-based social engineering that deceives employees using deepfake voice technology, this trend underscores the fragility of the national digital financial ecosystem. This situation reinforces the fact that web application security—including ERP systems—is becoming an increasingly critical aspect to address [3].

PT Tekno Konek Solusi's Weskonek ERP system is an integrated platform used to manage various corporate business processes, including financial management, customer data processing, operational transactions, and control of internal organizational activities. As a core system that centralizes data and business processes within a single integrated database, Weskonek ERP plays a strategic role

in maintaining operational efficiency and supporting accurate managerial decision-making. The complexity of the system architecture—which includes user authentication mechanisms, role-based access control (RBAC), integration between modules, and connectivity with the database—makes this system a representative case for analysis in the context of enterprise system security. The Weskonek ERP system was selected as the research subject based on several strategic considerations: the management of sensitive operational and financial data; the significant impact that a security breach could have on the company's business stability; and the fact that no security evaluation has ever been conducted using a structured methodological approach and vulnerability classification based on international standards. Security flaws within ERP frameworks pose severe risks, including data breaches, fraudulent transaction alterations, illicit privilege escalation, and operational downtime, all of which can culminate in financial detriment and reputational degradation. Consequently, conducting a comprehensive security assessment of the Weskonek ERP system represents a pivotal strategy to protect corporate assets and maintain business continuity.

In terms of novelty, this study offers contributions that distinguish it from general web application security research. For example, the study by Bregas et al. titled "Testing the Surabaya Social Services Agency Website Using Penetration Testing and the OWASP Top 10," focused on the Surabaya Social Services Department's website and employed the penetration testing method, which included the stages of information gathering, footprinting and scanning, vulnerability assessment, exploitation, and analysis and reporting, where the OWASP Top 10 2021 was used as the primary approach in evaluating system security [5]. However, this study tends to focus on the use of the OWASP Top 10 as the primary reference in the penetration testing process, without a more specific classification of vulnerabilities or an assessment based on quantitative data

In addition, another study titled "Why Vulnerability List Methodologies Matter (And why we trust CWE & OWASP)" states that CWE uses data from the National Institute of Standards and Technology (NIST), specifically through the National Vulnerability Database (NVD), which contains Common Vulnerabilities and Exposures (CVE) data. Each CVE is mapped to a specific Common Weakness

Enumeration (CWE) category. In contrast, the OWASP Top Ten focuses more on risk categories than on specific weaknesses or vulnerabilities, so in some cases, a single risk category may encompass more than one type of CWE [6]. Therefore, based on a comparison of these methodologies, it can be concluded that the CWE approach has proven to be more systematic, measurable, and empirically grounded in the process of identifying and prioritizing security weaknesses.

Given this situation, this study was conducted to analyze the security of the Weskonek ERP system and is expected to contribute to improving the security of the Weskonek ERP system as well as serve as a reference for future security evaluations of similar systems.

1.2 Problem Formulation

Based on this background, the research questions in this study are:

1. What is the severity level of the potential security vulnerabilities identified within the Weskonek ERP system based on penetration testing metrics?
2. How is the systematic process of vulnerability discovery and analysis executed in strict accordance with the structured phases of the Penetration Testing Execution Standard (PTES)?
3. How are the identified vulnerabilities classified using the Common Weakness Enumeration standard, and how are these vulnerabilities mapped to attack tactics and techniques within the MITRE ATT&CK framework?
4. What is the severity level of the vulnerabilities based on the Common Vulnerability Scoring System, and what mitigation recommendations can be provided to enhance the security of the Weskonek ERP system?

1.3 Problem Limitations

To ensure that this study remains focused and aligned with its established objectives, the scope of the study is limited as follows:

1. This study focuses on analyzing the security of the Weskonek Enterprise Resource Planning (ERP) system's web application, which is used by PT Tekno Konek Solusi.

2. The research scope is limited to the ERP functions and modules accessible via the web interface using a gray-box testing approach with a standard user account and no additional information; it does not include comprehensive testing of the company's hardware or internal network infrastructure.
3. The penetration testing phases conducted include intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting, in accordance with the PTES framework and the agreed-upon scope of testing.
4. Security vulnerabilities identified in this study are classified using the Common Weakness Enumeration (CWE) standard to systematically identify the types and characteristics of software weaknesses.
5. To evaluate the severity of identified security flaws, this study utilizes the Common Vulnerability Scoring System (CVSS) v3.1 framework. Rather than providing an exhaustive analysis of the mathematical formulas underlying manual CVSS calculations, this research focuses on employing the system as a practical mechanism to prioritize mitigation strategies according to risk exposure and potential impact.
6. This study does not involve the direct development or modification of source code but rather provides recommendations for improvements based on the results of the security analysis.
7. Testing was conducted in an environment that had received official permission from the relevant parties and was intended solely for academic purposes and to improve system security.

1.4 Goal

This study aims to:

1. Analyze the security level of the Weskonek ERP system through penetration testing.
2. Identify potential security vulnerabilities in the Weskonek ERP system.
3. Categorize the discovered system flaws utilizing the Common Weakness Enumeration (CWE) standard, subsequently correlating them to specific

adversarial tactics and techniques defined by the MITRE ATT&CK framework

4. To evaluate the severity of discovered vulnerabilities utilizing the Common Vulnerability Scoring System (CVSS) and propose actionable remediation strategies to enhance the security posture of the Weskonek ERP system.

1.5 Benefit

This study is anticipated to yield dual benefits across both scholarly and practical spheres. From an academic standpoint, it aims to enrich the existing body of knowledge within the cybersecurity domain, specifically by providing deeper insights into the practical execution of penetration testing under the PTES framework. In addition, this study can also serve as a reference for students or other researchers who wish to conduct similar research, particularly regarding the security analysis of web-based applications using the Common Weakness Enumeration (CWE) standard. It is hoped that this study will enrich the literature and broaden academic understanding of methods for identifying and classifying vulnerabilities in ERP systems.

From a non-academic perspective, this research provides practical benefits to PT Tekno Konek Solusi as both the developer and user of the Weskonek ERP system. The research findings can be used to determine the system's actual security level, identify security gaps that could potentially be exploited, and serve as a basis for decision-making regarding application security enhancements. Furthermore, the resulting recommendations can help the technical team strengthen the system to make it more resilient against cyberattacks, while also increasing user confidence in data security and company operations.