CHAPTER I INTRODUCTION

I.1 Background

In the digital era, cybersecurity has become a top priority for organizations. Cyber attacks such as data breaches and the exploitation of security vulnerabilities often threaten organizational websites, resulting in financial and reputational losses (Symantec, 2003). One effective method to identify vulnerabilities is by conducting a Vulnerability Assessment, which is a systematic process to find, classify, and evaluate weaknesses in information systems (Scarfone et al., 2008).

This research focuses on the application of the Vulnerability Assessment method on a website to analyze vulnerabilities, threats, and provide mitigation recommendations to enhance the cybersecurity resilience of information systems.

Most business processes and data are currently stored in computer systems. With increasing digitalization, this brings both benefits and risks to companies or organizations. A hacker can easily disrupt business processes or even steal important company and customer data (Rahman et al., 2021).

Websites are critical assets that store various sensitive information, such as user data, transactions, and internal operations. Threats to website security, such as Distributed Denial of Service (DDoS) attacks, SQL Injection, and data theft, can undermine the confidentiality, integrity, and availability of information (CIA Triad) (Stallings & Brown, 2018). Therefore, proactive measures are necessary to protect websites from these threats.

One of the approaches that can be taken to ensure website security is Vulnerability Assessment. This method includes the process of identifying security gaps, classifying the level of risk, and providing recommendations for remediation. Vulnerability Assessment not only helps to detect existing vulnerabilities, but also provides technical and strategic guidance to address these gaps before they are exploited by irresponsible parties (Riadi et al., 2020).

This research aims to apply Vulnerability Assessment to a website to identify potential vulnerabilities and assess the risks that may occur. The results of this research are expected to provide strategic mitigation recommendations to improve

the security posture of the website, so that the data and services remain protected and reliable (ENISA, 2023).

I.2 Problem Statement

The problems underlying this research are:

a. What security vulnerabilities exist on the website?
b. What are the risk assessment results of the identified vulnerabilities?
c. What are the recommended improvements to enhance website security based on the results of the Vulnerability Assessment?

I.3 Research Objectives

This research aims to:

a. Identify existing security vulnerabilities on the website through the implementation of Vulnerability Assessment.
b. Conduct a risk assessment of the identified vulnerabilities to determine the severity level and prioritize their handling.
c. Provide improvement recommendations to enhance the website's security posture based on the findings of the Vulnerability Assessment.

I.4 Research Scopes

The limitations of this research are as follows:

1. The research object is a cloned website.
2. The research focuses on website security aspects without covering other IT infrastructure.
3. The research is only conducted on the Frontend.
4. The method used is Vulnerability Assessment without any penetration testing or exploitation, consisting of scanning, analysis, and reporting phases.
5. The tools used include Nmap, Nessus, WPScan, OWASP ZAP, and Burp Suite.

I.5 Research Benefit

The expected benefits of this research are:

1. For Website Owners: To provide insights into the level of website security and the mitigation steps that need to be taken.
2. For Researchers: To deepen the understanding of VAPT methods and their implementation in website security systems.
3. For Other Researchers: To provide scientific references for research in the field of cybersecurity, particularly on the application of VAPT.