CHAPTER I
INTRODUCTION

1.1 Background

The rapid growth of internet accessibility has transformed how individuals access and exchange information. According to Statista (2025b), as of February 2025, there were approximately 5.56 billion internet users worldwide, accounting for 67.9% of the global population. In Indonesia, during the same period, there were 212 million internet users recorded (Statista, 2025a). Consequently, web applications have become the primary medium for public information exchange and administrative services.

The growing use of websites facilitates easier access to information, however not all information is freely accessible. Website security systems become important to protect against threats from cyber attackers (Hermanto & Haeruddin, 2022). The security level of a website also needs to be evaluated periodically to ensure compliance with security standards and to reduce the risk of cyberattacks that can occur at any time. It is important to remember that security testing must continuously reprioritize, as there are numerous ways to find security vulnerabilities, and organizations always have limited time and testing resources (OWASP, 2020b).

Based on cybersecurity monitoring results in March 2025 by the Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (ID-SIRTII/CC) and the National Cyber and Encryption Agency (BSSN), there were 371,189,964 traffic anomalies recorded, peaking on March 28, 2025, with 15,895,675 traffic anomalies. In addition, 68 suspected cyber incidents were identified, with the "Others" sector, dominated by the education sector, recording the highest number of incidents, namely 35 suspected incidents.

In the context of information security, the CIA Triad model, consisting of Confidentiality, Integrity, and Availability, serves as the primary principle for safeguarding data security. Data confidentiality is a very important aspect as it relates to the protection of information from unauthorized access, which is important for data and system owners. According to Surfshark (2025) report, Indonesia ranks 14th globally in terms of the number of data leaks, with a total of

177.2 million data leaks from 2004 to April 15, 2025. Failure to maintain confidentiality can lead to identity theft, fraud, legal violations, loss of public trust, financial damage, and reputational harm.

Websites may contain sensitive information, such as user data and personal information, which must have their authenticity protected. If the security of data confidentiality on the website is not properly maintained, vulnerabilities may arise that can be exploited by irresponsible parties to access the data, to the detriment of the data owner and the system itself. This principle is also reflected in Indonesia's Law No. 27 of 2022, Article 39 Paragraph 1, which states that "the controller of personal data shall prevent personal data from being accessed unlawfully."

XYZ University as one of the educational institutions in Indonesia, has implemented Information and Communication Technology (ICT)-based information systems to support various campus activities, one of which is XYZ Web Application, accessible via *aka.xyz.ac.id.* XYZ Web Application is a system designed to facilitate online academic administrative activities at XYZ University, such as curriculum and class scheduling, course registration, end-of-semester grade submissions by lecturers, printing of study results, and more. Given the importance of the data managed in this system, a data confidentiality security evaluation is required to ensure there are no vulnerabilities that could put data confidentiality at risk.

A data privacy security evaluation based on a structured and internationally standardized framework is required to ensure the security of web application data privacy. One commonly used framework is the Open Worldwide Application Security Project (OWASP), which provides security testing guidelines based on the most common risks in web applications, along with comprehensive testing tools and documentation.

Based on this review, this research conducts a security evaluation of data confidentiality on the XYZ Web Application system using the OWASP, focusing on authentication, authorization, session management, and and weak cryptography testing. This focus was chosen because these four aspects are directly related to the security of data confidentiality against the threat of unauthorized data access. The

purpose of this research is to identify and provide recommendations to address data confidentiality security vulnerabilities in the XYZ Web Application.

1.2 Research Scopes

To ensure that the research remains focused and does not deviate from its objectives, the following research scopes are established:

1. This research is based on security testing activities conducted during the author's internship at UPA TIK XYZ University. While the internship scope covered security assessments for 10 different university systems, this research specifically limits its scope to only two systems: XYZ and ABC Web Application.
2. The research is limited to the evaluation of data confidentiality, excluding the aspects of integrity and availability within the CIA Triad.
3. Security testing is conducted using the OWASP Web Security Testing Guide (WSTG), focusing specifically on authentication, authorization, session management and weak cryptography testing.
4. This research provides recommendations to address the identified data confidentiality vulnerabilities, but does not include their direct implementation in the system.
5. The testing technique applied is grey box testing, where the tester has partial knowledge of the system’s internal structure.

1.3 Research Questions

Based on the background described previously, the research questions addressed in this research are as follows:

1. What are the results of data confidentiality security testing on the XYZ Web Application?
2. What vulnerabilities related to data confidentiality are identified in XYZ Web Application, and what are the evaluation results?
3. What recommendations can be proposed to overcome data confidentiality security vulnerabilities in the XYZ Web Application?

1.4 Research Objectives

The objectives of this research are as follows:

1. To conduct data confidentiality security testing on the XYZ Web Application.
2. To identify and evaluate vulnerabilities related to data confidentiality security identified in the XYZ Web Application.
3. To provide recommendations to overcome data confidentiality security vulnerabilities in the XYZ Web Application.

1.5 Research Benefits

This research is expected to provide the following benefits:

1. Practical Benefits

   Provide recommendations that can be followed up to relevant stakeholders as a basis for overcoming data confidentiality security vulnerabilities in the XYZ Web Application.

2. Academic Benefits

   Become a reference for other researchers who are interested in the field of web application security evaluation, especially in the area of data confidentiality security using OWASP.