# CHAPTER I
# INTRODUCTION

## 1.1. Background

In the rapidly accelerating era of digitalization, information system security has become a primary priority for government institutions, particularly in sectors directly involved with data management and public communication. Today, government websites no longer function merely as platforms for information dissemination; they also serve as media for data storage, public services, and administrative management of government agencies [1]. As the dependency on web technology increases, the risks associated with cyber threats also escalate. Consequently, government institutions must undertake systematic efforts in security evaluation to ensure the integrity, availability, and confidentiality of the data they manage [2].

The 2020 Global Cybersecurity Index (GCI) report published by the International Telecommunication Union (ITU) placed Indonesia in 24th position out of 194 countries in terms of cybersecurity, a significant improvement from its 41st-place ranking in 2018 [3]. While this achievement indicates an increase in national cyber defense capacity, it does not automatically reduce the risk of attacks. According to the 2023 report from the National Cyber and Crypto Agency (BSSN), Indonesia experienced over 370 million cyber incidents in 2022, an increase of nearly 39% from the previous year [4]. Among all these incidents, the government sector was recorded as one of the most frequently targeted, primarily through techniques such as defacement, data breaches, DDoS attacks, and ransomware [4]. BSSN data also notes that the majority of cyberattacks against Indonesian government institutions exploit vulnerabilities in web applications, with SQL injection and Cross-Site Scripting (XSS) being the most dominant attack vectors [4]. This condition indicates that while cybersecurity awareness is rising, the implementation of web application security practices within government environments still needs to be strengthened.

The Department of Communication and Informatics (Diskominfo) of East Java Province is a vital institution responsible for managing information systems, public

data, and digital communication at the regional government level. As a central agency supporting the government's digital transformation, the security of Diskominfo's websites is a fundamental aspect of maintaining public trust and ensuring the continuity of public services [5]. Diskominfo East Java was selected as the research object for several strategic reasons. First, as the agency managing digital infrastructure for 38 regencies/cities in East Java, Diskominfo has a system complexity level representative of large regional government institutions. Second, the Diskominfo website serves as the primary portal for digital public services accessed by millions of East Java residents, making the impact of potential security vulnerabilities highly significant. Third, based on public information, Diskominfo East Java has not yet undergone a comprehensive external security audit using integrated international standards, allowing this research to provide valuable practical contributions. Vulnerabilities on government websites can lead to fatal consequences, such as operational disruptions, data theft, information manipulation, and even potential sabotage of regional government systems.

As part of the efforts to improve digital security within Diskominfo, one of the system development projects undertaken is the creation of the website for the Trenggalek Regional Forest Service Branch. This website serves as a medium for publishing activities, a communication tool, and an information service for the public regarding forest management in the Trenggalek region. The development of this website is a tangible representation of e-Government implementation in the regional forestry sector and a relevant object for security analysis. Through this website, the public can access information directly and transparently; however, the website also becomes a potential target for attacks if not protected by appropriate security mechanisms. Therefore, conducting a security analysis on websites under the auspices of Diskominfo is a critical step to ensure that public information systems operate securely, reliably, and in accordance with the principles of the Confidentiality, Integrity, and Availability (CIA Triad).

To thoroughly assess the security level of government websites, this study integrates several internationally recognized security standards and frameworks. A

multi-framework integration was chosen because each framework has a focus and strength that complements the others in the web application security evaluation process. The OWASP Top Ten is used to identify the most common and dangerous types of vulnerabilities in web applications, such as injection, broken authentication, cross-site scripting (XSS), and security misconfiguration [6]. This framework was selected as it has become a global industry standard and is regularly updated based on actual vulnerability data found worldwide. The OWASP Application Security Verification Standard (ASVS) is used as a reference to evaluate the fulfillment of application security controls based on standards set by OWASP [7]. ASVS provides a comprehensive checklist that allows for a structured assessment of security control implementation, ranging from basic to advanced levels. Additionally, the OWASP Web Security Testing Guide (WSTG) serves as a technical guide for conducting methodological web application security testing. WSTG provides detailed testing procedures for every vulnerability category, including techniques, tools, and expected results to ensure consistency in the testing process [8].

This study utilizes NIST SP 800-115 as the primary guideline for performing security testing. The guide covers four main stages Planning, Discovery, Attack, and Reporting making the testing process more systematic, measurable, and aligned with internationally recognized methodological standards for information security [9]. The NIST framework was chosen because it has proven effective in the context of government system security testing and provides an accountable audit structure. To provide an objective and quantitative risk assessment, every identified vulnerability is subsequently evaluated using the Common Vulnerability Scoring System (CVSS) to measure severity based on impact and exploit complexity [10]. CVSS provides standard metrics on a scale of 0–10, allowing for the prioritization of mitigation based on actual risk levels.

This research applies a grey-box testing approach, where the tester has limited access to the system being tested. This approach was chosen because it represents realistic real-world conditions, where an attacker does not have full access to source code or server configurations but can exploit flaws from both external and internal sides

[11]. With this method, the testing is capable of identifying relevant vulnerabilities from both an external user perspective and internal threats comprehensively. Grey-box testing also allows the researcher to understand the system architecture to a limited extent, enabling more effective testing compared to pure black-box testing while maintaining the objectivity required in the security audit process.

In terms of novelty, this study offers significant added value that distinguishes it from common security evaluation practices. Based on field observations, most government agencies, including Diskominfo's internal security teams, generally focus only on the OWASP Top Ten framework during security assessments. Such an approach is generic and does not cover aspects of security control verification, structured testing, or quantitative risk assessment. This research presents a more comprehensive and methodical approach by integrating the OWASP WSTG as a detailed technical testing guide, OWASP ASVS as a standard for application security control verification, NIST SP 800-115 as a systematic testing methodology framework, and CVSS to provide numerical risk scores for each vulnerability finding. This integrated approach has not been widely implemented by cybersecurity teams within regional government environments, including Diskominfo. Most internal security audits still consist of simple checklists without quantitative risk assessments or standardized control verification. Therefore, this research is expected to serve as a reference in improving the effectiveness, accuracy, and depth of government website security analysis.

Overall, the results of this research are expected to provide three main contributions. First, academically, this study enriches the literature regarding the application of OWASP and NIST security standards within the context of regional government institutions in Indonesia. The multi-framework integration approach used can serve as a methodological reference for similar future research, particularly in the domain of public sector web application security. Second, practically, the testing results and technical recommendations can be directly utilized by Diskominfo East Java to enhance its institutional cyber resilience. The research report will present a structured mitigation roadmap, prioritized by risk level, which can be implemented

gradually according to available resource capacity. Third, from a policy perspective, this research can serve as a reference for other government agencies in Indonesia to strengthen their digital security systems [12]. The developed evaluation framework is adaptive and replicable for security audits of other regional government websites, thereby contributing to the overall improvement of national cyber resilience.

## 1.2. Problem Formulation

Based on the background provided above, the problem formulations for this research are as follows:

1. What are the specific vulnerabilities present on the website of the Communication and Informatics Department (Diskominfo) of East Java Province, particularly within the subdomain of the Trenggalek Regional Forest Service Branch?
2. How can the application of the OWASP WSTG and ASVS frameworks assist in the detection and verification of security vulnerabilities on the website?
3. How can the NIST SP 800-115 framework be utilized to guide the security testing process in a systematic and measurable manner?
4. How can the severity level of each identified vulnerability be classified using the Common Vulnerability Scoring System (CVSS)?

## 1.3. Research Objectives

The research objectives serve as the answers or targets to be achieved in a study. The specific objectives of this research are:

1. To identify security vulnerabilities present on the website of the Communication and Informatics Department (Diskominfo) of East Java Province, specifically within the subdomain of the Trenggalek Regional Forest Service Branch.
2. To measure the compliance level and resilience of web application security based on the OWASP WSTG and ASVS standards.
3. To implement the NIST SP 800-115 framework as a systematic guide in the website security testing process.
4. To assess the severity of vulnerabilities using the Common Vulnerability Scoring System (CVSS) as a foundation for determining remediation priorities.

5. To provide technical and strategic recommendations for risk mitigation and the enhancement of cybersecurity within regional government environments.

### 1.4. Research Benefits

The benefits of this research are as follows:

1. To provide a scientific contribution to the field of cybersecurity within the government sector by integrating the NIST SP 800-115 methodology, OWASP ASVS verification standards, and the CVSS scoring system within a grey-box testing scheme.
2. To assist the Department of Communication and Informatics (Diskominfo) of East Java Province in comprehensively mapping security gaps and formulating precise mitigation strategies based on risk-level priorities.
3. To produce a systematic and measurable web application security evaluation framework that can serve as a reference or be replicated by other government agencies to strengthen the national digital security ecosystem.
4. To support the enhancement of regional government information resilience in protecting the confidentiality of public data.

### 1.5. Research Limitations

To ensure the research remains focused and to prevent any undue expansion of the scope, the following limitations have been established:

1. This research focuses exclusively on security testing of the official website of the Department of Communication and Informatics (Diskominfo) of East Java Province, specifically the subdomain for the Trenggalek Regional Forest Service Branch. The testing does not encompass internal network infrastructure, server-side hardware, or any other information systems outside the specified domain.
2. Security testing is conducted using a Grey-Box Testing approach, utilizing the NIST SP 800-115 framework as the primary workflow guide (covering planning, discovery, attacking, and reporting). The technical procedures for performing penetration testing on each security flaw refer to the OWASP Web Security Testing Guide (WSTG).

3. The evaluation of web application vulnerabilities is performed based on the OWASP Application Security Verification Standard (ASVS) Level 2 to verify the existing security controls within the application.
4. The severity assessment of vulnerabilities utilizes CVSS v3.1 (Common Vulnerability Scoring System). In this study, CVSS is intended as an instrument to prioritize mitigation steps based on the discovered impact and risk levels; therefore, the researcher will not provide an in-depth discussion or analysis regarding manual CVSS calculation formulas.
5. The final results of this research are limited to the identification of security flaws, risk analysis, and the provision of technical mitigation recommendations to the administrators. This study does not include the system remediation phase, code patching, or direct server reconfiguration.