CHAPTER I
INTRODUCTION

1.1. Background

The rapid advancement of information technology over the past decade has transformed the way organizations conduct operations and deliver services. Web applications have become a fundamental component of digital transformation due to their capability to support real-time communication, business process automation, and cross-platform public service delivery [1]. Along with the increasing pace of technological transformation, cyber security threats have also evolved into more complex and dynamic forms, characterized by increasingly organized and unpredictable attack patterns.

Cyber security has become a crucial aspect in the digital era because nearly all economic activities, governmental operations, and public services depend on online infrastructure. Websites that manage sensitive data and provide public services face a high risk of becoming targets of cyber attacks [2]. These threats require every organization, including government institutions, to implement effective and adaptive security strategies to protect their digital assets [3]. According to the Verizon Data Breach Investigations Report (DBIR) 2024, web applications remain one of the most common attack vectors, with 68% of security breaches involving human error and system misconfigurations [4]. This condition indicates that security evaluations of web applications, particularly those managed by government institutions, have become an urgent necessity that cannot be overlooked.

At the national level, the National Cyber and Crypto Agency (BSSN), in the Indonesia Cyber Security Landscape 2023 report, recorded more than 400 million detected traffic anomalies, with the government sector, critical infrastructure, and digital public services becoming the primary targets [5], [6]. Specifically in East Java Province, the East Java Communication and Informatics Office (Diskominfo Jatim) reported a significant increase in cyber threat activities targeting regional government digital infrastructure [7]. These data indicate that regional government web application systems still contain potential vulnerabilities that must be addressed seriously through systematic and standardized security evaluation mechanisms. One of the regional

government institutions directly facing these challenges is the Communication and Informatics Office (Diskominfo) of East Java Province.

The Communication and Informatics Office (Diskominfo) of East Java Province is a Regional Government Organization (OPD) responsible for managing public communication, Information and Communication Technology (ICT) infrastructure, cryptography, and information security within the regional government environment [8]. Currently, web application security evaluations within Diskominfo are conducted periodically using the OWASP Top 10 standard. However, this approach has not yet been integrated with a quantitative risk assessment system and comprehensive threat modeling. This limitation makes it difficult to determine mitigation priorities, understand exploitation contexts in real attack scenarios, and objectively measure the impact of vulnerabilities on the continuity of public services.

One of the strategic web applications managed by Diskominfo of East Java Province is the MAJADIGI (Masyarakat Jawa Timur Digital) portal, accessible through https://majadigi.jatimprov.go.id. MAJADIGI is an integrated digital service portal developed by the Government of East Java Province to provide various services and information to the public in an integrated manner. As the primary portal connecting millions of East Java residents with various regional government services, the potential impact of security vulnerabilities within MAJADIGI is extensive, ranging from personal data leakage, disruption of public service availability, to legal implications for the regional government as regulated under the Personal Data Protection Law (Law No. 27 of 2022) [9] and the Electronic-Based Government System (SPBE) regulation under Government Regulation No. 95 of 2018 [10].

To comprehensively evaluate the security of MAJADIGI, an approach that goes beyond automated scanning is required. The Vulnerability Assessment and Penetration Testing (VAPT) approach is a security methodology that combines two phases, namely Vulnerability Assessment (VA) to broadly identify security vulnerabilities, and Penetration Testing (PT) to simulate real-world attacks in order to examine the extent to which these vulnerabilities can be exploited [11]. Rohmaniah et al. (2025) demonstrated that OWASP Top 10-based VAPT was capable of identifying and exploiting vulnerabilities such as clickjacking, improper HTTP-to-HTTPS redirection, directory listing, and sensitive information disclosure. However, the study was conducted in a private company web application testing environment and did not

integrate attacker behavior-based threat modeling [1]. Similarly, Ibrahim et al. (2022), who implemented VAPT using a combination of network-based and web application vulnerability scanners on a private company website, did not utilize MITRE ATT&CK or CVSS v3.1, resulting in qualitative risk assessments that were difficult to use as a measurable mitigation prioritization basis [12].

To deepen the analysis and understand the exploitation context realistically, this research integrates the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework, which is a global knowledge base regarding attacker behavior based on observations of real-world attacks that maps the tactics, techniques, and procedures (TTPs) used by attackers [13]. Wahyudi et al. (2025) demonstrated that the use of MITRE ATT&CK in penetration testing assists in modeling potential attacks more accurately through a multi-stage approach that includes information gathering, exploitation, and post-exploitation. However, the study was only implemented in a laboratory environment using intentionally vulnerable systems rather than real web applications operating in production environments, and it did not apply the OWASP Top 10 standard [14]. Ajmal et al. (2023) developed a MITRE ATT&CK-based adversary emulation approach for endpoint security evaluation and showed that 78% of attacks successfully bypassed endpoint security controls such as antivirus software. Nevertheless, the study did not focus on web application security and did not integrate OWASP Top 10 or CVSS v3.1 in its risk assessment process [15].

In addition to threat modeling, an objective and measurable risk assessment is required so that the evaluation results can serve as a basis for mitigation decision-making. This requirement can be fulfilled through the Common Vulnerability Scoring System (CVSS) v3.1, an industry standard managed by FIRST to provide quantitative severity scores for vulnerabilities on a scale of 0.0 to 10.0 [16]. Putra and Soewito (2022) emphasized the importance of CVSS in measuring the security performance of government employee management websites and identified high-severity vulnerabilities with the potential for sensitive civil servant data theft. However, the study relied solely on automated scanning without manual penetration testing stages and without integrating OWASP Top 10 or MITRE ATT&CK, resulting in limited vulnerability validation and exploitation context analysis [17].

Based on these previous studies, a significant research gap can be identified.

Existing studies tend to be partial in nature, where some only apply VAPT without MITRE ATT&CK-based threat modeling, others implement MITRE ATT&CK but not on real-world web applications, while some utilize CVSS without adequate manual exploitation stages. This gap motivates the present research to develop an integrated security evaluation framework that combines VAPT, OWASP Top 10:2021, MITRE ATT&CK, and CVSS v3.1 to evaluate vulnerabilities and assess risks within the MAJADIGI web application managed by Diskominfo of East Java Province. The developed framework adopts a grey-box testing approach, which is more realistic because it reflects actual conditions in which attackers possess partial information about the target system [18]. The results of this study are expected to provide practical guidance for Diskominfo of East Java Province in strengthening the security of its web applications, while also serving as a reference for other regional government institutions in implementing standardized, measurable, and effective security evaluation practices.

1.2. Problem Formulation

Based on the above background, the formulation of the problem in this study is as follows:

1. What are the security vulnerabilities contained in the MAJADIGI (https://majadigi.jatimprov.go.id) Diskominfo web application of East Java Province based on VAPT and OWASP Top 10:2021 classification?
2. How is the mapping of attack tactics and techniques (TTPs) against vulnerabilities found based on the MITRE ATT&CK framework, as well as scores based on CVSS v3.1 assessments?
3. What are the appropriate mitigation recommendations for each vulnerability in the MAJADIGI web application based on the risk priority level obtained from the results of the CVSS v3.1 assessment?

1.3.Research Objectives

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

1. To identify and classify security vulnerabilities in the MAJADIGI web application managed by Diskominfo of East Java Province using the

Vulnerability Assessment and Penetration Testing (VAPT) method based on the OWASP Top 10:2021 categories.

2. To map the identified vulnerabilities into attack tactics and techniques using the MITRE ATT&CK framework, as well as to assess their severity levels and risk priorities using CVSS v3.1.
3. To develop prioritized mitigation recommendations based on CVSS v3.1 assessment results and MITRE ATT&CK mapping in order to improve the security of the MAJADIGI web application.

1.4. Research Benefits

The benefits of this research are as follows:

1. To contribute to the academic literature regarding the integration of the VAPT, MITRE ATT&CK, and CVSS v3.1 frameworks in the security evaluation of government web applications, while also serving as a methodological reference for future research in public sector web application security.
2. To provide security evaluation results that include a list of validated vulnerabilities, CVSS v3.1-based risk scores, MITRE ATT&CK-based attack scenario mappings, and prioritized mitigation recommendations as a basis for decision-making in improving the security of the MAJADIGI web application.
3. To provide a reference for implementing standardized web application security evaluations using the integrated frameworks of VAPT, OWASP Top 10:2021, MITRE ATT&CK, and CVSS v3.1.

1.5. Research Limitations

In this study, the author requires limitations to avoid broadening the discussion. The limitations of this research are as follows:

1. Testing was conducted using a grey-box testing approach on the primary domain https://majadigi.jatimprov.go.id, with limited access to publicly accessible URLs and registered user credentials, without access to source code, administrator credentials, server configurations, or subdomains outside the scope agreed upon with Diskominfo of East Java Province.
2. Vulnerability validation was conducted in a non-destructive manner and did not include user data exfiltration, post-exploitation activities, denial-of-service

attacks, or social engineering techniques, thereby ensuring that the availability and integrity of active services were not disrupted.

3. This research covers the stages of vulnerability identification, classification based on OWASP Top 10:2021, mapping into attack tactics and techniques using the MITRE ATT&CK framework, and risk assessment using the CVSS v3.1 Base Score. This study does not include the technical implementation of remediation by the related institution.
4. Testing was conducted within a predetermined and mutually agreed period; therefore, the research results reflect the security condition of the MAJADIGI web application during the testing period and do not guarantee security conditions outside the specified timeframe.