CHAPTER I
INTRODUCTION

1.1. Research Background

The growth of technology has encouraged educational institutions to digitalize on web based information systems to support academic and administrative processes (Perdianza et al., 2024). The digital evolution has changed the way an institution should operate, creating interconnected digital ecosystems that can manage everything from student enrollment, e-learning, e-library, e-repository, e-journal, e-payment, and other services. However, this transformation also grow together with the attack for cybercriminals, turning educational institutions into a perfect targets due to their sensitive and important data. Cyberattacks on educational institutions should be treated as a critical concern, as they store important personal data (Perdianza et al., 2024).

According to the report from Check Point Research 2024, in the third quarter of 2024, the average weekly cyberattacks per organization reached 1.876 attacks per week, it's reflecting 75% increase compared to the same period in 2023 and 15% increase from the previous quarter. The Educational and Research sector become the main target of cyber criminals, because this sector has receiving around 3,828 attacks per week. This indicate that this sector needs attention to securing the digital assets that retain important data (Check Point Research, 2024).

Universitas Pendidikan Ganesha, is an educational institution based in Singaraja, Bali. This university has implemented Information and Communication Technology (ICT) to support various academic activities. The digital ecosystem of this university involves several critical information systems such as academic management, smart payment, administrative systems, and the other information systems. In addition, to handling sensitive data and information system in Undiksha also provide feature that allows user-generated content, such as search forms, data submission forms, and comment or discussion forum, and other interactive components. These features are involving direct user input, which potential entry point for injection based attacks.

The system that considered vulnerable to Cross-Site Scripting (XSS) attacks if it show certain characteristics, such as improper input validation mechanism that fail to handle user-input properly, improper output encoding that allows malicious scripts to be executed in the browser and server, presence of unfiltered parameters, implementation of dynamic content generation without security control, and absence of Content Security Policy (CSP) headers that prevent script execution. Research by (Arimbawa, 2023) identified the presence of reflected Cross-Site Scripting (XSS) vulnerability in XYZ system, with medium risk level calculation using OWASP Risk Rating Methodology. And based from the information gathering with Infrastructure, Networking, and Security Division, there are several Cross-Site Scripting (XSS) vulnerabilities that have been reported before, but not across all in the information systems within the university.

The Academic Supporting Unit for Technology, Information, and Communication or UPA TIK Undiksha serves as the technical unit that have responsible for developing and managing these technology under direct supervision of the Rector and coordinating with the Vice Rector for Academic Affairs. UPA TIK Undiksha is formed by several divisions, each division has their own responsibility and function in serving user needs. In the use of networking technology, there is Infrastructure, Network, and Security division that is holds crucial responsibility for designing, managing, and developing networks and computers infrastructure throughout the university environment. Given the critical responsible of these systems in university operations and the sensitive data that they process, regular security assessments is important to evaluate whether the defense systems can effectively defend against potential attacks from unauthorized parties.

Based on data from 2024 IT Security Assessment (ITSA) annual monitoring report published by the Direktorat Operasi Keamanan Siber (Directorate of Cyber Security Operations), under the Deputi Bidang Keamanan Siber dan Sandi (Deputy for Cyber and Cryptographic Security Operations) of Badan Siber dan Sandi Negara (BSSN, Indonesia's National Cyber and Crypto Agency), ITSA was conducted on 462 application accross 131 institutions. The result shows that there

are 1,913 vulnerabilities discovered with varying risk levels, with Cross-Site Scripting (XSS) maintains its position as the third highest risk vulnerability category. This category of vulnerability indicates that malicious injection code based still massively exist.

From the OWASP TOP 10 2021 data, Cross-Site Scripting (XSS) vulnerabilities are categorized under A03: 2021-Injection, maintaining its position as the third most critical web application risk out of 10 in global. This classification indicates that injection based attacks in modern web applications, may affecting educational institution. In a university environment, XSS attacks pose a serious threat through the theft of administrator sessions, account takeover scenarios, and manipulation of academic data that can compromise the integrity of educational information systems. Interconnected information systems in Universitas Pendidikan Ganesha have potential to compromise several critical services, affecting thousands of users and exposing sensitive academic and personal data to unauthorized access, so vulnerability assessments are critical to ensuring and maintaining the security of Information System in Universitas Pendidikan Ganeha. Since the researcher did not obtain access to internal penetration testing reports records from UPA TIK, previous research academic research in the same topic used as an reference to understanding the occurence of security vulnerabilities within information systems in Universitas Pendidikan Ganesha. A previous study by (Arimbawa, 2023) performed penetration testing in two information systems at Universitas Pendidikan Ganesha and identified several vulnerabilities, including Reflected XSS. This finding indicates that XSS vulnerability have previously observed in the web-based information systems. However, bacause of the available reference only covered limited systems, further testing is needed to identify whether similar XSS vulnerabilities may also exist in other information systems within the defined scope of this research.

Penetration testing holds crucial role in ensuring security of the information system by enabling academic institutions to detect and address security vulnerabilities before external exploitation occur. Without regular security assessments, university may facing risks of data breaches, financial losses,

reputational damage, and others. With regular security assessments ideally conducted quarterly or biannually to maintain effective defenses strategy against potential vulnerabilities (Elson, 2024). Therefore, this research will implement the Penetration Testing Execution Standard (PTES) methodology with specific focus on identify Cross-Site Scripting (XSS) vulnerabilities and combination of grey-box testing and semi-targeted and black-box with blind testing scope apprroach. The selection of XSS as the primary vulnerability focus is justified by its ranking as the third highest risk vulnerability category according to BSSN 2024 data, its persistent classification in OWASP TOP 10, and its relevance to educational institutions due to interconnected information system. PTES methodology is chosen over other frameworks such as NIST SP 800-115, OWASP Testing Guide, or OSSTMM because it provides detailed and structured penetration testing approach that addresses critical gaps identified in literature review, specifically the lack of structured exploitation procedures, absence of standardized risk assessment methodologies, and unorganized reconnaissance processes that characterize most previous studies. Meanwhile combination of grey-box testing and black-box testing approach is chosen because the researcher have partial knowledge about the internal systems, how the business process of the systems, and have an authorization as a student who have the legal account. This research also combining with vulnerability assessment using OWASP Risk Rating Methodology to calculating objective risk classifications that facilitate prioritized remediation planning for enhancing Universitas Pendidikan Ganesha's web based information system security against XSS threats.

1.2. Problem Identification

Universitas Pendidikan Ganesha has implemented web-based information systems to support various academic and administrative processes. However, there has no been dedicated vulnerability assessment that focused on identify Cross-Site Scripting (XSS) vulnerabilities. Cross-Site Scripting (XSS) is still one of the most prevalent and critical web vulnerabilities according to the OWASP Top 10 2021 report and BSSN data in 2024, with significant potential to impact academic web systems.

Based on this issue, the following research questions are formulated:

1. How can XSS vulnerabilities in Universitas Pendidikan Ganesha's web-based information systems be identified and assessed using the Penetration Testing Execution Standard (PTES) methodology?
2. How significant is the risk level identified through OWASP Risk Rating Methodology in assessing XSS Vulnerabilities of the information systems in Undiksha?
3. What solutions and recommendation can be apply to fix the identified XSS vulnerabilities and improve the university's web application security?

1.3. Research Objectives

The research objective of this research are as follows:

1. To identify the vulnerability or potential vulnerability of the information system in Universitas Pendidikan Ganesha.
2. To evaluating the risk level of discovered vulnerabilities.
3. To provide prioritized recommendations based on calculated risk levels to enhance the university's web application security.

1.4. Research Limitations

To ensure that this research is focusing on the objectives, the scope of this research are:

1. Limited to web-based information systems under the *trusted domain* that are accessible by Undiksha students, lecturers, and employees. The systems selected must support login functionality, search form input, publicly accessible user input form, and other user-generated input form (comment, feedback, discussion form, posting, and complaint form.
2. Because of the limitation of user access, this research is combine grey-box testing approach and black-box testing approach. Grey-box testing approach is used for the system that are accessible by student user. For the black-box testing approach is used for testing the information system that are unaccessible by student user (accessible by lecturer or

employee only).

3. Penetration testing conducted on the Cross Site Scripting vulnerability risk that have medium, high and critical risk level to ensure focused analysis on security threat that pose significant potential impact.
4. Penetration testing conducted on the ports 80 and ports 443 for HTTP and HTTPS.
5. Target testing scope focused on the information system that have critical business impact for its user.
6. In this research, the researcher is using external or outside institution's network.
7. In this research, the researcher only calculating the risks and provide solutions based on the calculation, but did not make any direct improvements of the information system.

1.5. Research Significances

The significances of this research are involving several parties such as:

1. Theoretical significance:

   This research is expected to contribute to the field of information system security by provides valuable insights, knowledge, methodologies, and solutions for mitigating potential security threats. It serve as the foundation for future studies, helping other researchers to explore methodology in penetration testing. In addition, it will enhance the understanding of the issue about vulnerabilities within information systems in an educational institution.
2. For the institution (UPA TIK):

   The result of this research is expected to support UPA TIK in identifying and understanding Cross-Site Scripting (XSS) vulnerabilities that exist within the tested information systems. Through the delivered Proof of Concept (PoC) document, UPA TIK can obtain technical evidence of the identified vulnerabilities, including the affected systems, vulnerable parameters or input points, payload behavior, exploitation evidence, risk level, recommended remediation steps, and verification step after

patching the vulnerabilities. This research and Proof of Concept (PoC) report can help the institution prioritize vulnerability handling based on the OWASP Risk Rating result and support the technical team in planning appropriate mitigation and preventive strategies.

3. For the users of the system:

   This research aims to protect users credentials by ensuring that security mechanisms are in place to prevent unauthorized access, identity theft, and data breaches. By enhancing system security, users can interact with the system securely, knowing their personal and confidential information is secure