## *ABSTRACT*

*According to the OWASP Top 10 Most Critical Web Application Security Risks, Cross-Site Scripting is ranked third among injection attack types. In the process of developing an Academic Administrative Support website at Institution XYZ, it is necessary to conduct Security Testing to address the high-potential Cross-Site Scripting vulnerability, as this vulnerability has a high potential for data theft and manipulation, which could lead to sensitive data being compromised. If this were to happen, it could significantly damage the credibility of the institution. This study is conducted to identify the Cross-Site Scripting vulnerability on the Administrative Support website at Institution XYZ and to mitigate it through security testing. The identification of the Cross-Site Scripting vulnerability was carried out using the OWASP ZAP tool, with the vulnerability identified in the "warn" parameter. The exploitation process was executed to confirm the Cross-Site Scripting vulnerability, utilizing tools such as XSStrike and Burp Suite. The outcome was the successful exploitation of the target website using various injected payloads. In conclusion, it can be deduced that the "warn" parameter inadequately applies input filtering and validation to prevent XSS effectively. As a result, mitigation measures are necessary for the website. The mitigation process involves adding a Content Security Policy (CSP) header, utilizing the htmlspecialchars() function, and implementing Secure Socket Layer (SSL) for enhanced security. Post-mitigation results demonstrate the absence of detected popup confirmation dialogs and a reduced ability to modify error alerts. Consequently, the mitigation process has effectively reduced security vulnerability.*



***Keywords: Cross Site Scripting, Website, Mitigation, PTES.***