ABSTRACT

The development of information technology has grown rapidly in line with its increasing user base. The utilization of information technology in the form of *website*s is widely used by various parties. XYZ University is an educational institution that uses a *website* for academic purposes, teaching and learning activities, and various internal entity needs. One of the *website*s used by XYZ University aims to accommodate proof of payment for laboratory activities for students to obtain certification in the XYZ Faculty. Along with the benefits brought by technology advancements, there has been an increase in security attacks using various threat techniques against *website*s by malicious parties with the intention of harming the *website* owners and users. Therefore, vulnerability testing is needed to identify security loopholes on the XYZ Faculty *website* using the PTES method. This testing involves several tools such as SQLMap, Burp Suite, jSQL Injection, and Havij. The security vulnerabilities on the *website* are analyzed to determine the mitigation steps. The results of the security testing on the academic support *website* of XYZ Institution using the SQL Injection method showed that none of the four tools used found any vulnerability *parameter*s on the *website*, indicating no data manipulation occurred through SQL Injection attacks. Further research can involve using various, accurate, and comprehensive tools to identify security vulnerabilities and employing different methods to diversify the research results. Additionally, regular *website* maintenance should be conducted to minimize security loopholes.

Keywords - **exploitation, vulnerability, PTES, mitigation**