ABSTRACT

In the current era, the growth of technology is getting faster, especially in the education sector. Of course, these need to pay attention on information security that can minimize the risk, protect the data, and information from threats or attacks. One of the attacks is a SQL Injection which targets database server by injecting malicious SQL statements then database executes the query. This research conducts to determine the condition of existing security vulnerabilities from SQL Injection attacks on the academic program selection website in an institution and knowing the mitigation on the website. This test is carried out because the website has never been tested for security during the development, there was no security testing process conducted and immediately entered the Go-Live stage, so there may still be security vulnerability, such as data leaks on the website or unauthorized data modifications, which could lead to user data/information misuse, a decrease in user trust, and potential damage to the reputation of XYZ Institution. This research applies the Penetration Testing Execution Standard (PTES) methodology, utilizing various testing tools at each stage. The testing involves exploiting each link with predefined parameters. The result of the SQL Injection attack testing using five testing tools that carried out shows that there is no any security vulnerability, hence the implementation of security mitigation is not necessary.

Keywords: ***Website, PTES, SQL injection, security mitigation***