IMPLEMENTATION OF PREPARED STATEMENTS ON INPUT FORMS TO PREVENT SQL INJECTION IN CAMPUS FACILITY LOAN WEB APPLICATIONS

Name	: Wulan Febri Enjelina
Student ID	: 6404221123
Supervisor	: Agus Tedyyana,S.Kom.,M.Kom

ABSTRACT

Web applications for managing campus facility loans continue to grow due to the need for fast and integrated services. However, most facility loan web applications are built without implementing adequate security mechanisms on input forms, making them vulnerable to SQL Injection attacks. This vulnerability can lead to loan data being manipulated and leaked. To prevent SQL Injection, this research currently focuses on building a campus facility loan web application from scratch, by implementing comprehensive statements across all input forms, not just specific modules. This study aims to develop a web application for borrowing campus facilities and test the effectiveness of implementing prepared statements to prevent SQL injection attacks. The goal of this study is to create a web application for borrowing campus facilities that is not only operational but also offers a high level of security. The method used is software engineering, which includes requirements analysis, system design, implementation, and testing. System testing was conducted through functional testing (black-box testing) to ensure proper system operation, security testing using SQLMap to assess resilience to SQL injection attacks, and User Acceptance Testing (UAT) to assess user acceptance of the application. The results show that increased revenue leads to increased consumption, although not proportionally. Security testing proves that implementing prepared statements is effective in preventing SQL injection attacks, resulting in the application being well-received by users.

Keywords: *prepared statements, SQL injection, web application security, campus facility management.*