ABSTRACT

The security of electronic payment systems through payment gateways is crucial in supporting the integrity and trust in online financial transactions. In today's digital era, game top-up websites have become an essential component in the gaming industry, providing a platform for users to conduct financial transactions. However, these platforms often become the target of attacks by irresponsible parties, especially through SQL Injection attack techniques.

Therefore, this study aims to analyze and detect potential vulnerabilities to SQL Injection attacks on electronic payment systems. The research methodology involves penetration testing using SQL Injection payloads with Data Manipulation Language (DML) and Data Definition Language (DDL) statements. The aim is to understand how the application responds to attacks that try to manipulate data in the database and whether the application has adequate security layers to protect the database structure.

The test results show that the system has a fairly effective security mechanism in detecting and preventing SQL Injection attacks. Although there were some successful attacks, indicating the presence of security gaps, most attacks failed thanks to the existing security mechanisms. These results provide in-depth insights into security vulnerabilities and the necessary mitigation measures to strengthen the system's security.

Keywords: *Data, Database, SQL Injection, Cybersecurity.*