SECURITY ANALYSIS OF WEBSITE LOGIN FROM SQL INJECTION ATTACKS USING FILTERING TECHNIQUES

Student Name	: Syahbani Kurnia Putra
Student ID Number	: 6404201003
Supervisor 1	: Rezki Kurniati, M.Kom
Supervisor 2	: Nurmi Hidayasari, ST., M.Kom

ABSTRACT

In the current digital era, information security is crucial and takes top priority in website development. The most common security threat to websites is SQL Injection, where hackers or attackers manipulate SQL statements in the login form to forcibly breach or gain unauthorized access. The method employed involves implementing Filtering Techniques in the login form to filter and validate user inputs. This technique aims to prevent special characters that can be exploited by hackers or malicious individuals for SQL Injection. Test results indicate a significant difference before and after applying Filtering Techniques. Prior to implementing filtering techniques in the login form, there was a vulnerability gap in the financial recording website's login form, allowing successful entry into the system during SQL Injection attacks. After applying the combined 3 filtering techniques in the login form namely Input Validation, Escape, and Prepared Statements followed by retesting with 10 bypass attempts, the use of Filtering Techniques proved effective in minimizing SQL Injection attacks on the website's login form.

Keywords :Information Security, SQL Injection Attack, Filtering Techniques.