E-PINTER WEBSITE SECURITY ANALYSIS AGAINST SQL INJECTION AND XSS ATTACKS

Name	*:Josua Karlos Manuel*
Student ID	*:6404211060*
Supervisor	*:* Rezki Kurniati, M.Kom

ABSTRACT

Website security is a crucial component in maintaining the integrity, confidentiality, and availability of data against various cyber threats. E-Pinter, which serves as an online licensing service platform, is potentially vulnerable to SQL Injection and Cross-Site Scripting (XSS) attacks that could compromise the system and the information stored within it. This study aims to evaluate the security level of the E-Pinter website against these two types of attacks. The methodology includes both manual and automated testing using penetration tools to identify security vulnerabilities. SQL Injection testing is conducted by injecting various payloads into input parameters to assess the possibility of database manipulation, while XSS testing involves inserting malicious scripts into unvalidated inputs to evaluate the potential exploitation of the user interface. The test results reveal several vulnerabilities that could be exploited by attackers, posing risks of data breaches and system disruptions. As a mitigation measure, this study recommends implementing prepared statements to prevent SQL Injection attacks and using the htmlspecialchars() function to counteract XSS attacks. The implementation of these strategies is expected to enhance the security of the E-Pinter website, protect user data, and reduce the risk of future exploitation.

Keywords: SQL Injection, Cross-Site Scripting, Website Security, Penetration Testing.