ABSTRACT

Simulation of Security Threats On Web-Based Applications

by

GIRINDRO PRINGGO DIGDO
10108262

Web applications are applications that are accessed using a web browser via a network such as Internet or Intranet. Web applications are becoming popular due to ease of availability of client applications to access it. The ability to update and maintain web applications without distributing and installing software on thousands of client computers is a key reason for its popularity.

However, the impact of convenience, the web application is also likely from the threat of outsiders who are not responsible. The threat is most common in Web applications is a threat to the database. Such threats is SQL Injection.
SQL Injection is a method that allows the threat to execute client database via the URL and gain access for important information. Moreover, Web applications are also vulnerable to the threat of Cross Site Scripting.

Cross Site Scripting is a threat method that forced for displaying web sites that run malicious code on a user's web browser.

To cope with these threats, we need a defense mechanism against the threat posed. Validating Input is a method of testing the input received by the application of the standards that have been defined.

Based on the testing that was conducted concluded that the method is built Validating Input can be a defense mechanism against SQL Injection and Cross Site Scripting.

Keywords: SQL Injection, Cross Site Scripting, Validating Input.