Implementation PDO Parameterized Query to Prevent SQL Injection

Abstract

SQL injection is one of threat to the application connected to the database. By implementing SQL injection attacker can gain full access to the application or database so that it can remove even significant data irresponsibly. Applications that do not validate the user’s input appropriately make them vulnerable against SQL injection. Various methods have been developed to prevent SQL injection each with advantages and disadvantages. Implementation of PDO Parameterized Query properly can prevent SQL injection. PDO not only provides a method to facilitate the implementation of parameterized queries but also makes the code is portable because the PDO can be used on multiple databases. This paper describes the results of research on the use of PDO Parameterized Query on scheduling application. By using PDO Parameterized Query on this application, making it is not vulnerable to attack that caused by SQL injection.

References


Index Terms

Computer Science  Information Sciences

Keywords

PDO, parameterized query, SQL injection