***Abstract*— SQL Injection attacks are one of the common securityrisks that occur in applications. SQL Injection cases can lead to data and sensitive information leaks, and even potentialapplication data deletion. This research examines the effectiveness of using parameterized queries in the Go programming languageas a method of prevention against SQL Injection attacks. Go provides the feature of parameterized queries by using placeholders such as question marks (?) or parameter names. Parameterized queries separate input values from SQL statements and are executed securely by the database driver. In this study, the use of parameterized queries in Go is evaluated to prevent querymanipulation by users in the application. The research is conducted by testing four HTTP request operations: GET, POST, PUT, and DELETE, both before and after the use of parameterized queries. The testing results, based on Acunetix Web Vulnerability scanning, prove that all testing operations arevulnerable to SQL Injection when not using parameterized queries, while successfully mitigating SQL Injection attacks whenusing parameterized queries in Go.**