***Abstract*— Serangan SQL Injection merupakan salah satu risiko keamanan umum yang terjadi pada aplikasi. Kasus SQL Injection dapat menyebabkan kebocoran data dan informasi sensitif, dan bahkan potensi penghapusan data aplikasi. Penelitian ini menguji efektivitas penggunaan parameterized queries pada bahasa pemrograman Go sebagai metode pencegahan terhadap serangan SQL Injection. Go menyediakan fitur kueri berparameter dengan menggunakan placeholder seperti tanda tanya (?) atau nama parameter. Kueri berparameter memisahkan nilai masukan dari pernyataan SQL dan dieksekusi dengan aman oleh driver database. Dalam penelitian ini, penggunaan query berparameter di Go dievaluasi untuk mencegah manipulasi query oleh pengguna dalam aplikasi. Penelitian dilakukan dengan menguji empat operasi permintaan HTTP: GET, POST, PUT, dan DELETE, baik sebelum maupun sesudah penggunaan kueri berparameter. Hasil pengujian, berdasarkan pemindaian Kerentanan Web Acunetix, membuktikan bahwa semua operasi pengujian rentan terhadap SQL Injection saat tidak menggunakan kueri berparameter, sekaligus berhasil memitigasi serangan SQL Injection saat menggunakan kueri berparameter di Go.**