Preventing user web accounts from SQL injection attacks

Abstract:

Attack injection in web applications allows malicious users to obtain unrestricted access to private and confidential information. SQL injection is ranked at the top in web application attack mechanisms used by hackers to steal data from organizations. Hackers' can take advantages due to flawed design, improper coding practices, improper validations of user input, configuration errors, or other weaknesses in the infrastructure. This paper proposes a methodology for the detection of exploitations of SQL injection attacks. When the user submits the SQL query at the runtime, the query has to be parsed by the independent service for the correctness of the syntactic structure and user data. This approach is to prevent all forms of SQL injections, independent of the target system, independent to platform and Backend DB server.