

I used regex to search for specific patterns associated with “OR = value=value” SQL injection attacks. I did this by first converting the query to a string, queryStr, declaring a match variable to store the match, and defining an injectStr variable to represent all possible SQL injection patterns of 0-9=0-9 or any combination of lowercase, uppercase, or numerical characters. Then I used the regex\_search() method to pass these variables through an if statement to determine whether there is a match between the query and the known injection patterns. If a match is found it will enter into the if statement, output to the console that a potential SQL injection attack has been detected, and will return false for the run\_query function performed. If no match is found it will proceed as usual returning the results of the query.