ACTIVIDAD - MySQL injection

Abraham Cepeda Oseguera
A00827666

MySQL injection es uno de los ataques más comunes en la red y se el sistema es vulnerable las consecuencias pueden ser catastróficas. Es por esto por lo que es de suma importancia proteger las *queries* a la API de este tipo de ataque.

En cuanto a la actividad, se puede observar que el código original es vulnerable a este tipo de ataque, ya que se puede insertar código de MySQL. Por ejemplo, si se hace la *query* "http://100.24.228.237:10027/user/abrahamcepedao' OR '1=1" la respuesta es el listado de todos los usuarios, ya que 1=1 siempre será verdadero. De esta manera, se pueden insertar códigos maliciosos que se ejecutan en la base de datos que, incluso, pueden llegar a borrar bases de datos enteras.

Por lo tanto, resultó empírico modificar el algoritmo de la API para que detecte cuando la *query* incluye código MySQL y así impedir que este se ejecute. Para lograr lo anterior, primeramente, se realiza un "*replace*" de las comillas en caso de estar presentes en la *query* por comillas dobles con el objetivo de anular su propósito. Además, la *query* a la base de datos se reestructuro para que el texto que corresponde al usuario solo funcione para encontrar al mismo y así no se ejecute de ninguna forma código MySQL que pudiera estar embedido.