Vulnerability analysis

The spiderman application performs a SQL query on a villains database. The query is on the basis of a search string, and it uses a regular expression. The query is vulnerable to SQL injection, because the villain name is unsafely concatenated to the SQL code. To test this, we can search (with browser or Burp) a single quote character, which leads to a suspicious "Invalid query" message. Moreover, searching for two single quote characters leads to a normal "(no villain with such a name)" message, which tells us that no SQL error has occurred. Indeed two single quotes are interpreted as a single literal quote in SQL strings.