CS 3339 Lab 8

Part 1: How can you best prevent SQL injection attacks?

Sanitize user input, make sure characters are correctly escaped when queries are generated from strings. Even better would be to use parameterized SQL queries that entrust the database engine to generate the correct statement. In both cases, database management systems need to be kept up to date for greatest protection against possible attacks.

Part 3

Username : haha

Password : ‘ ‘ or 1=1

Part 4

Messages : ‘ OR type=type#

Part 5

Password : ‘ ‘; DROP TABLE members

Part 6

The checklogin.php file has been changed to used parametrized SQL queries instead of dynamic SQL queries. The database implementation automatically quotes the prepared statements, removing the risk of an injection attack