Xuan(James) Zhai

CS3339 Lab

April 23th, 2021

CS 3339 - Lab 8 - Lab Report

1: How can you best prevent SQL injection attacks?

You can use some input testing to prevent injection attacks at the beginning, or you can set up some privilege requirements for modifying the database so that not all the users can, for example delete the database, easily. Moreover, there are some tools that can help you prevent SQL injection attacks by like identify queries.

2: What input did you use to complete this action? Specify your inputs on each field

Input username: john

Input password: ‘1234’ OR 1=1

Although the mysql will compare and identify the password, the query condition “OR 1=1” will let the password-check always be true.

3: What input did you use to complete this action? Specify your inputs on each field

Input search: 1234%’ OR 1=1 OR’

The first part which is a arbitrary search item. The OR 1=1 let the “where” comparison always be true. The last, OR’, is just make sure the injection will not cause a syntax error. Since the “where” is now targeting to every item in the table, it will just return all of them, regardless whether they are in private or not.

4: What input did you use to complete this action? Specify your inputs on each field

Input username: john

Input password: 1234; DROP TABLE members;

The “1234;” will run the query for login-check. Although the login request may be denied, it will also run the second query which will drop the members table.

5: Prevent SQL injection

Source found: <https://websitebeaver.com/prepared-statements-in-php-mysqli-to-prevent-sql-injection>