IMPORTANT!!!! Read this First

This project asks you to develop attacks and test them, with our permission, against a target website that we are providing for this purpose. Attempting the same kinds of attacks against other websites without authorization is prohibited by law and university policies and may result in *fines, expulsion,*

Target Website

A startup named Bungle! is about to launch its first product—a web search engine—but their investors are nervous about security problems. Unlike the Bunglers who developed the site, you took CS 558, so the investors have hired you to perform a security evaluation before it goes live.

Bungle! is available for you to test at **http://cs558web.bu.edu/project2/**.

In addition to providing search results, the site accepts logins and tracks users' search histories. It stores usernames, passwords, and search history in a MySQL database.

essary to complete the project.

In addition to providing search results, the site accepts logins and tracks users' search histories. It stores usernames, passwords, and search history in a MySQL database.

Part 1. SQL Injection

Your first goal is to demonstrate SQL injection attacks that log you in as an arbitrary user without knowing the password. In order to protect other students' accounts, we've made a series of separate login forms for you to attack that aren't part of the main Bungle! site. For each of the following defenses, provide inputs to the target login form that successfully log you in as the user "`victim`" and a brief (2-3 sentences) explanation of why your attack works:

1.0 No defenses. [6 points]
Target: `http://cs558web.bu.edu/sqlinject0/`

1.1 Simple escaping. [6 points]
The server escapes single quotes (`'`) in the inputs by replacing them with two single quotes.

Target: `http://cs558web.bu.edu/sqlinject1/`

***Complete part 1.0. No worries if you don't get to part 1.1**

I encourage you to use google as a resource! Read up on SQL attacks. Computerphile also has another video demonstrating an attack that's useful as well.