General Tips

Here are some general tips for the whole project.

- Because the website is black-box (you don't have the source code), you will need to perform SQL injection attacks without seeing the query and the response. We recommend first writing out what you think the backend query is, with blanks where you think user input is substituted. Next, think about where on the website the user input comes from. Finally, write out an injection attack and enter it where you think the user input comes from. This may take some trial and error before you succeed.
- The backend for this project exclusively uses single quotes for SQL queries.
- It is possible to select constants in SQL rather than selecting column names. For example, `SELECT 1, 'foo', 'evan'` will return a single row with 3 columns, with values of `1`, `'foo'` and `'evan'`. You may find this useful if you can guess the format of the rows being selected in one of the server's SQL queries.
- Consider looking into the `UNION` keyword to return the result of two queries without usage of a semicolon.