# Development

The site inspection is a web application. The design is developed with HTML, CSS Languages also used Bootstrap. And the backend is developed with PHP Language and Laravel framework. To prevent SQL injection it is replacing (‘) to (\‘). So, it is not getting any SQL injection attack at all.

# UI and Software design

There has 4 roles (Site\_Inspector, Admin, Manager, User). Only Admin can register others person. Here Site\_inspector can create multiple Site Inspection Forms. There has inspection date, Inspector Name, Site Name, Inspection Type, Title, Description, Severity (High, Medium, Low), Corrective Measure, Whom To Contact fields. All the forms can be seen at once in all inspections tab. He can also edit and delete inspections form there. In the site\_inspector dashboard, there has total number of inspections.

# Database

For the database site inspection is using mysql database. There has 2 tables. They are users and inspections. In the users table there has id, firstname, surname, username, email, gender, role, password. And in the inspections table there has ID, date, inspector\_name, site\_name, inspection\_type, title, description, severity, measure, Contact. The mysql database is running on localhost. And in the code the database connection is inside include/connection.php.

# Log of Testing done

PHP echo gave me a lot help during building the website. Whenever I was not getting expected values then I was using php echo. Such as while registering users POST, inspection form saving, editing inspections, editing registered users, also sometimes used it to check sql query for SQL injection and so on. When website is finished I removed those log codes.