# CSC206 Group Lab

## Specifications

Purpose: The purpose of this project is to implement a website that allows users to access files based on their permissions to read or write to those files. The user will then be able to download the files, or upload additional files, depending on whether they have read permissions or read-write permissions to the directory those files are stored in. To implement this, it is necessary to have persistent logins, which necessitates some sort of database that stores user information (email, password, and folder permissions). The website should also use secure coding practices to prevent common vulnerabilities like SQL injection.

Expected input: The user will input their email and password to gain access to the download/upload page of the website. The user can then upload a file if they have the appropriate permissions.

Expected output: The website will present the download/upload file page upon successful login or will otherwise notify the user that their credentials are invalid. The website will permit downloading of the appropriate files, depending on user permissions.

## Team Members and Contributions

Adrian Zebrowski – Login system, database containing user info and permissions, download page, documentation

Rene Pazitny – File upload functionality (extra credit portion), documentation

Sean McDonald – No contribution

## Progress Log

12/01 – Initial setup, database configuration, login page implementation (Adrian Zebrowski)

12/02 – Download page implementation, login testing, download permissions testing for all users (Adrian Zebrowski)

12/04 – Upload functionality implementation, upload permissions testing for all users (Rene Pazitny)

12/08 – Final testing and documentation (Adrian Zebrowski, Rene Pazitny)

## Results

The project fell slightly short of initial expectations. Due to scheduling constraints and the complete absence of one group member, we did not move forward with more advanced security features such as password lockout after multiple attempts.

## Bugs

None found (yet).

## Defense Strategies

The SQL database is queried only through a specific module that is designed to query SQL databases securely, no raw user input is passed directly to the database (prevents SQL injection).

File access is permissions based – files that a user does not have permissions to read are not displayed.