Completed:

Removal of Insecure Search Bar:

- There existed an excess search bar that was not properly connected and had a vulnerability to code injections due to unsanitized inputs

Login Security

- Allowing only a certain number of login attempts per IP address before a short lockout then after a number of lockouts having a 24 hour lockout
- Giving less specific error messaging on a wrong login attempt
- OAuth logins only through UA system emails that are on the whitelist so that only approved or Blount UA students can access the student features

Input sanitization:

- Properly escaping user input where needed
    - PHP function htmlspecialchars
- Pages that required input sanitization:
    - Booking
    - Rideshare
    - Log-In

Parameterized procedure calls:

- Per the cyber reminders at the beginning of the semester, procedure calls to the mySQL server were parameterized
- User inputs used in these parameters (such as names and emails) were sanitized through adding escape characters to instances of single quotes and enforcing pattern matching where applicable