1. We did not consider timezone difference, so this version does not support precision of long-distance traveling.(E.g. the user requests a ride in LA, but the driver is in Durham).

2. We have too many db operations, which may make the server overload if there are too many users accessing at the same time.

3. We use a personal account email with an app password, but it is not fast enough for serving a large number of users.

4. No string length check in ride request or editing， if the user types in an extremely long string, the error would happen.

5. When diver edit and driver register are filled in the blank, it will crash directly.

6. Database queries transfer to the user by plain text. Users could see database information when the error happens, which may be seen and used by attackers.

7. The URL after login is not protected(need an interceptor), if the user directly accesses the URL of the homepage, they can actually do it.

8. Password is not encoded which may easily being attacked by hacker, and this should be changed to tokens in the future.

9. We use request sessions to store some user information. Although this will make our server run more faster than those which store and query it in the database, we found that there exists potential problems. For example, if the user1 open another window and just login as user2, the session info will be changed, and this means currently the other function can have the privilege for user2. This is a tricky danger we found in testing.