PROJ4 – Security Audit

# **PART A**

1. **Check final application in a Desktop version of Chrome & Firefox + IOS and Android phones**

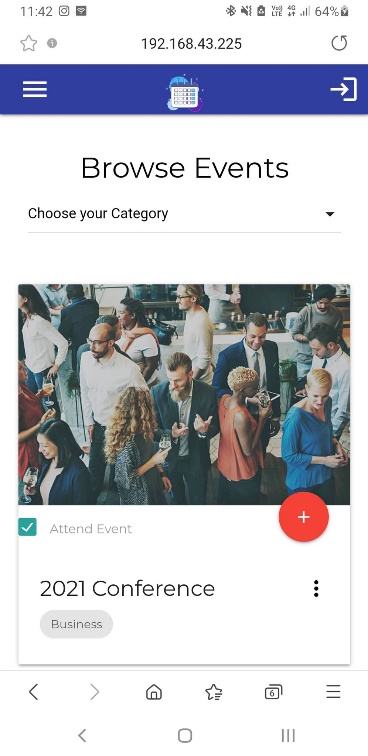
Final Applications are located at the below URLs:

Normal app: <https://malloriecini.com/>

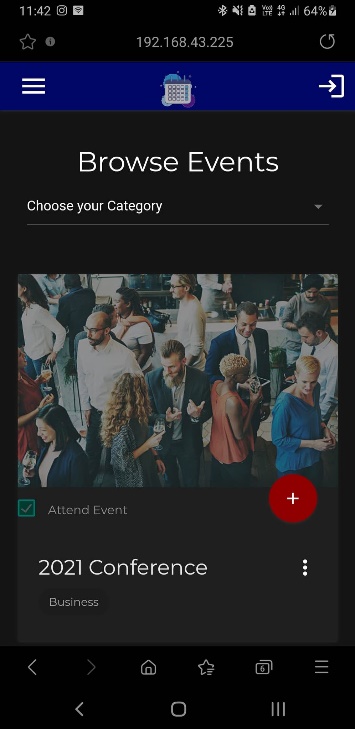
Admin app:

### Android

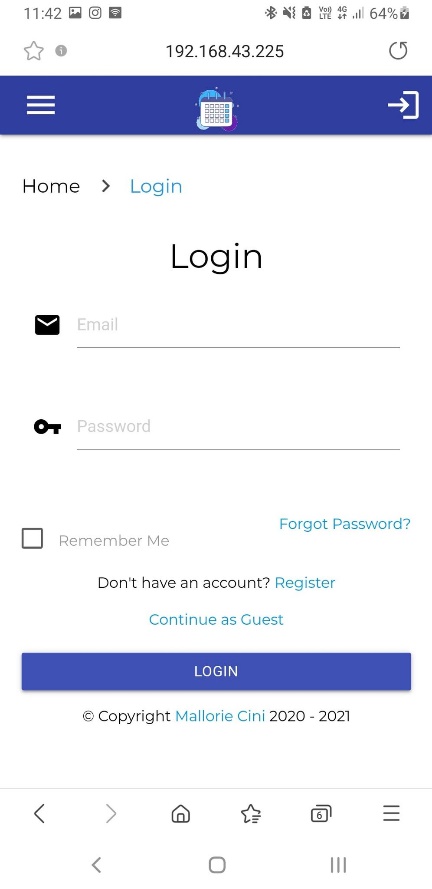
Home



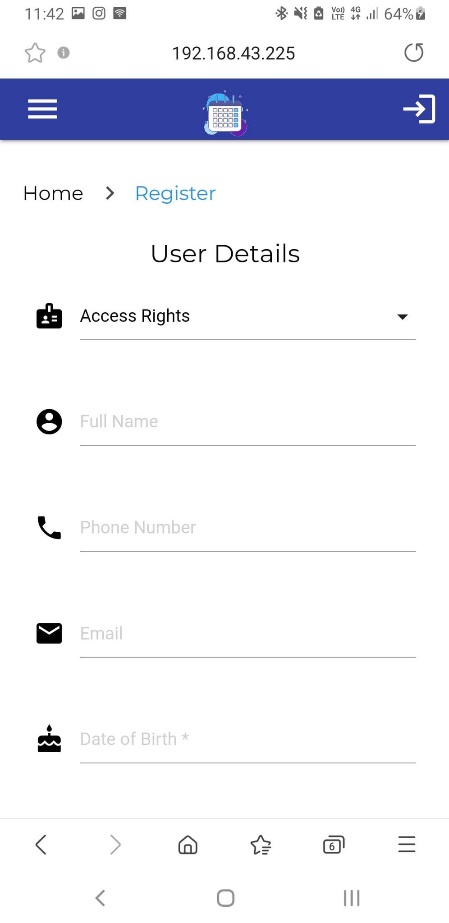
Dark Mode from system colours



Login



Register



### iOS

Home

Login

Register

1. **Bring UX2, PROJ2 & PROJ3 together in one .zip, write a README describing installation for operations staff**

Github Link: <https://github.com/theavidcoder24/eventee2>

Zipped Files Link:

1. **Include in the README all the technologies used in the app, places where they were used and versions you recommend**

The README.md is within the root of the directory which is also in the GitHub Repository.

<https://github.com/theavidcoder24/eventee2>

1. **Confirm functionality in relation to plan PROJ1 highlight areas that changed, or were not implemented.**

Completed and Functional

* Users can register successfully and is implemented
* Users can login successfully and is implemented
* Only users with access rights that are labelled “Admin” can login successfully to the admin panel which is implemented
* Is\_logged\_in? (GET): 202 Success
* logout (GET): 202 Success
* Create Events (POST): 202 Success
* Display Events (GET): 202 Success
* Fill Events Update (GET): 202 Success
* Update Events (POST): 202 Success
* Delete Events (POST): 202 Success

Not Implemented

* User specific events added to their user id profile

1. **Write a roadmap section that confirms areas of development going forward. What bugs do you want to fix or functionality to extend?**

In future developments I will plan to make the application display notifications that will alert the user should they choose to set reminders about the events. The ability to upload a user profile image will also need to be implemented in the future updates of the application. A future implementation will let a user assign events to their user id so that they can see the events they want to attend.

# **PART B**

1. **Secure app by resetting/removing admin passwords**User

Email: tracy@email.com

Password: User1

Admin

Email: derek@email.com

Password: admin123

1. **Remove localhost from referrer security, add hosting domain referrer**(Insert picture of it gone or commented out)
2. **Remove log data & test data from app**

Empty SQL database located in api/sql named “emptyeventee2.sql”

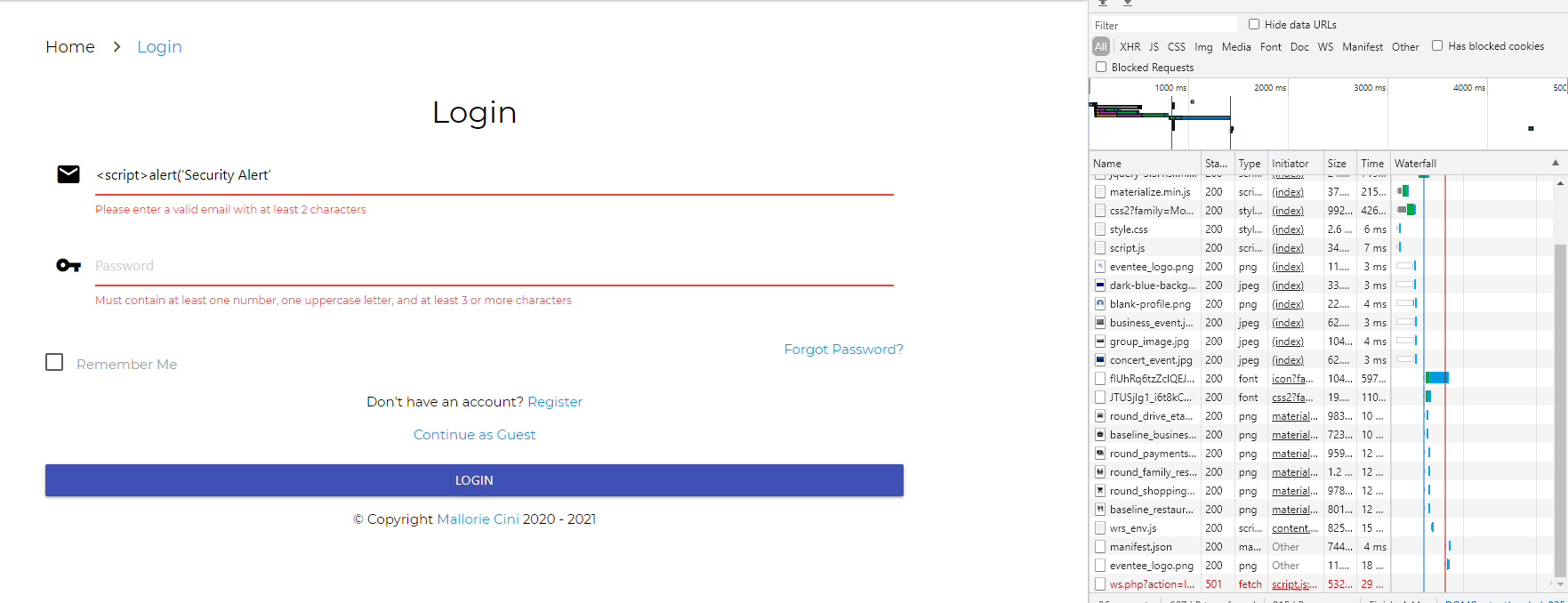
1. **Reset rate limits to once every .5 seconds & a maximum of 500 requests**

Option to switch back to 1000 requests for PROJ2 by uncommenting code + on line 53 added reset rate limits to once every .5 seconds

1. **Test with out of bounds data like negative numbers, Inject <script>alert(‘Security Alert’);</script> Update or delete on IDs that don’t exist**

Negative number:



Injection script alert:

Update on or Delete ID that doesn’t exist:

When the option to update or delete event appears there is no input field that the use can access to change the ID for update and as for delete method the user only has to click the one trash button to delete and it’s only on the same line as the event there’s no way to access the ID only in the console log does it show it.

1. **Screenshot results of 10 above and suggest a remedy**

Validation blocked the injection therefore no remedy needed e.g., empty input fields)

