Project assignment: 3

Security analysis

In the Security part, we already implemented hashed and salted password to enhance the security of storing passwords, prepared statements to prevent SQL injections and input sanitization to ensure the user input remains separate from the code. We will explain every section below.

Hashing and salting the password

For saving our password in the database we are using a hashing algorithm which hashes a password plus its random generated salt a few hundred times. While the user registers their password for a new account, the password will be sent to the server and the password will be hashed. After that, salt is produced using 16 bytes array of the password that are already made. This procedure makes a password become more secure even though some passwords may be the same password, but a different hash. For all of passwords, the hashed product and salt are stored in the database so that it can be checked if, whatever the input is, it is a correct password or not. There is a slight security concern however, as we right now do not securely transmit the password from the input field to the servlets. This can be solved by making use of other encryption methods like http certificates.

Prepared statements

Prepared statements are one of the methods to execute querying data in and from the database efficiently without any SQL injections. This also helps in concurrency issues, since prepared statements use a read and write lock before committing.

Input sanitization

Input sanitization is used to prevent malicious data from being processed by an application. It also involves removing and encoding potentially harmful data that could be used for cross-site scripting (XSS), SQL injection or other attacks.

Testing

General Overview

The pages are well structured and provide a clear navigation system. Using bootstrap for responsive design, the UI looks clean and intuitive for both web browsers and phone. The navigation provides clear links to various sections of the website and the buttons provide clear context on its functionality. For the back end, most if not all major query methods have a test inside a test folder, which is located in in src\test\java\attribute_queries_tests, with all the intended behaviour explained.

Testing the methods

To start all system functionalities, we start from the register and login page to determine if the user is a committee or a player. After we can go to the dashboard page for the committee or player. Every person who logs in can also log out.

From there, we can access many things such as challenges, leaderboards, or team page which everything works correctly.

In the challenge page we try the method of the submission using any picture and all of them are functionally well.

For the leaderboard page in the user, we can see the rank from 1- until maximum team. Other than that, the committee can make the leaderboard visible or not.

Testing the user stories (implemented so far)

1. As a participant, I want to be able to sign up for RIAlly so that I can join the treasure hunt.
   - We made a registration page for users where they can fill in their information and make their own account. With that account they can login to the website and participate in RIAlly. We paid attention to minimize user errors by showing visible alerts like input boxes turning red when a user makes an error like wrong password/student number for example.
2. As a participant, I want to be able to join a team so that I can collaborate with others and solve puzzles together.
   - We implemented a randomized join link with 7 random characters which helps the users join on the same team. We tested it by making two accounts. One of the accounts was a team captain and the other account joined via the join link provided for that specific team.
3. As an organizer, I want to be able to create slots for a team so that participants can collaborate.
   - We implemented this by having the created teams go through the committee to get approval. If the team gets approved, the captain will be able to share the join link with users who they want to be part of the team.
4. As an organizer, I want to upload and change puzzles and challenges per location so that participants have content and can compete.
   - We implemented an easy way for organizers to add, edit and remove puzzles and challenges with simple buttons. Adding locations, challenges and puzzles is found from the same page but editing an individual challenge or puzzle will need the organizer to click on the part they want to edit, and it will navigate them to another webpage where it is possible to edit and or remove the specific puzzle/challenge.

5. As a participant, I want to be able to access location-based puzzles once I reach a specific location so that I can solve challenges specific to that area.
   - We implemented an easy way for participants to navigate the locations with accordions. Under these accordions are challenge cards that, when pressed, will take the participant to that challenge's specific webpage where the participant can submit the answers for it by uploading images/videos.

6. As a participant, I want to be able to submit pictures and/or videos for puzzles, challenges, and bonus points so that I can earn points for my team.
   - Participants can navigate to a specific puzzle or challenge page and upload a picture/video and submit it. The submission will go to the organizers side for grading, and they decide how many points will be rewarded for the users.
7. As a participant, I want to be able to access the puzzles that are relevant to my current progress so that I can continue to solve challenges.
   - Users can check out what is available to them in the challenges page that can be accessed both via the navbar and via the dashboard. The puzzles will be in the top-most accordion in the challenges page.
8. As an organizer, I want to be able to have an overview of submissions so that I can grade them and award points.
   - On the organizer page, there will be submissions page which can see which team are already submit their puzzle/challenge/crazy88. We also plan to add extra implementation for comment on their work.
9. As a participant, I want to be able to see the scoreboard so that I can monitor our performance.
   - We implemented a scoreboard which shows the ranking, team names, and points of the teams. The scoreboard can be toggled visible and hidden by the committee.
10. As an organization, I want to be able to control whether or not the scoreboard is public so that I can decide how much information to share with participants.
    - On the organization page, there is a button to switch whether the scoreboard is visible or not.
11. As a participant, I want to be able to see my individual progress and scores so that I can track my own performance.
    - Users can see their stats once they have logged in. The statistics will be shown on the dashboard.
12. As an organizer, I want an overview of nongraded submissions so that I can prioritize grading.
    - Organizers can check out all the submissions of crazy88s, puzzles, and challenges on the submissions page. Here each category has tabs for graded and ungraded submissions.
13. As an organizer, I want to be able to view teams and participants so that I can keep track of them.
    - We implemented a table on the team-approve page which consists of the captain, team name, and a button to remove the team. We consider the organizer can remove/ disband the team because there might be possible team names that are considered inappropriate, or the captains are having trouble adding the right persons to their teams.
14. As an organizer, I want an overview of submissions so that I can keep track of the progress of teams and participants.
    - Organizers can check out all the submissions of crazy88's, puzzles, and challenges in the submissions page. Here they have tabs to check what is graded and what is ungraded for each category.
15. As a participant, I want to be able to easily navigate the platform and find what I need so that I can focus on solving puzzles and challenges.
    - We implemented in the user Dashboard page which help the user can focus on the challenge/puzzle/crazy88 during that time.

16. As an organizer, I want to be able to send messages/notifications to participants so I can provide updates about the treasure hunt.
    - We designed a webpage for the organizers to post announcements regarding new challenges, updates, new grades for teams, some of them being automatic upon creating a new grade for example. But due to lack of time, we abandon the idea and focus more on the core functionalities.
17. As a participant, I want to be able to access my team's score quicker so that I can adjust my strategy when needed.
    - We still need to improve the dashboard because we did not finish the implementation of the score on the user dashboard which can be seen quicker than navigating to the scoreboard.
18. As a participant, I want to be able to see why my submission failed/passed.
    - We included a comment field for organizers to give out comments along with grades for submissions that participants submitted. In these comment fields the organizers can explain why the submissions have failed/passed. However, we did not have time to make this functional.
19. As an organizer, I want to be able to create accounts for other organizers.
    - The organizers already have accounts so that accessing the website is more efficient
20. As a participant, I want to be able to receive notifications about new puzzles and challenges so that I don't miss any opportunities to earn points for my team.
    - We did not implement this part due to lack of time and we needed to focus more on the core functionalities.
21. As an organizer, I want a help section with hints and tips for participants so that they can get assistance when needed.
    - The hint button is already implemented in the individual challenges page which the committee does not need to approve of. The hint will show after the user presses the hint button, which in turn will send and the committee will notice which teams are using the hint on the specific challenges/puzzles/crasy88 and thus cannot receive maximum points anymore.
22. As a participant, I want to be able to access a help section with hints and tips so that I can get assistance when needed.
    - We implemented the hint button under the explanation of the challenge which hides the actual hint of the challenge. If the button is pressed, the hint will show to the user. After the hint button is pressed, the committee will notice that hint button has been used being used so the team that pressed it cannot have full score on the challenge/puzzle/ crazy88 anymore.
23. As a participant, I want to be able to communicate with my team members through the platform so that we can coordinate our efforts.
    - We decided not to implement this part because we consider the participants already recognize their team members before the game starts.