Revised Business Requirements Document:

Dbate

Prepared By: Red Team

Group Members:

Christian Flores-Rogel	**013924454 (Team Leader)**
Deivis Leung Liang	**014110497**
Luis Meza	**014325959**
Keanna Mae Vitug	**014699514**
John Cayton	**014108690**

Professor: Vatanak Vong

Date: November 1, 2018

Table of Contents

1. Document Revision History

Date	Version Number	Document Changes
9/28/2018	1.1	Initial Draft
10/06/2018	1.2	Second Draft
10/08/2018	1.3	Final Draft
11/01/2018	2.0	Revised Draft

2. Introduction

2.1. Project Summary

2.1.1. Objectives

The overall goal in developing this single page application is to create a platform for its audience to improve their debating skills. Dbate will allow users to communicate through a chat system that uses game-like functionalities.

2.1.2. Background

The purpose of Dbate is to allow users to share and expand their debate skills. By being given a unique prompt taken from a database of questions that include a variety of topics, users will be given the opportunity to expand their personal knowledge and learn better improvisation skills.

2.2. Project Scope

Our initial system will be based on a single page application that will primarily support the two latest version of Google Chrome (Version 69.0 and Version 68.0). The scope of the initial data will be: Geography, Role Permission, Security, and IP Range. The web application will only be available in all of North America (Canada, United States, Mexico) in all of the available cities and states of the countries in addition to being distributed in the English language for our initial release as proposed by the client. For the role functionality, we will have a user, administrator, and system administrator. Each of these roles will have certain rights and inherit rights from the role below it. The user has access to the basic functionalities of the web app. Administrator inherits from the user role and is able to create or delete new user accounts. The system administrator inherits powers from the administrator role and has the ability to delete or create new administrator accounts. The scope of our security for user accounts primarily consists of protecting user passwords and account authentication. If the user forgets their password, they are required to answer three security questions that they input during registration. The IP range will include those available in North

America. For example, the three largest countries of North America have their own IP ranges with the United States covering IP addresses from 1.22.56.0 to 223.197.44.239, Canada with IP addresses in 2.17.218.0 to 217.221.47.95, and Mexico with IP addresses in 2.20.70.0 to 216.251.76.254.

3. Core Feature Requirements

3.1. Registration

3.1.1. Functional

3.1.1.1. User Registration

Description: Users will be able to create an account by inputting the required information.

Business Rules:

1. The information users must input a valid email (username), password, date of birth, city, state, and country in order to create their account.
2. Upon registering, users will be required to answer three security questions.
3. If a username is already in the system, it cannot be used registered by a new user.

3.1.1.2. Administrator Registration

Description: An administrator can create a user account for a user by inputting the required information.

Business Rules:

1. A valid email (username), date of birth, city, state, and country must be provided by the administrator when creating an account for a user.
2. An administrator must give the user a randomly created password with 3 randomly chosen security questions and answers.
3. An existing username in the system cannot be used to create a new account.
4. The user will have to create a new password and answer 3 new security questions when they login for the first time.

5. Administrator accounts cannot be made by other administrator accounts.

3.1.1.3. Terms of Service

Description: A requirement that asks our users whether they accept our End-User License Agreement (EULA) when they try to access our system.

Business Rules:

1. Before being able to use our system, a user must consent to our active EULA.
2. Users will be unable to use the system without agreeing to the EULA.
3. A EULA can only be added, updated, or deleted by a system administrator, and there can only be one active EULA at a time.

3.1.2. Non Functional

1. It should take less than 4 seconds for a user's information to be registered into our database after they have completed the registration process.
2. Registering for an account must be user-friendly, simple and concise such that around 95% of users are able to make an account without assistance.

3.1.3. Pass/Fail Scenarios

3.1.3.1. Pass

1. If a user or administrator inputs the correct data, a normal user account should be created.
2. If a user agrees to the EULA, they should be able to access and use our system.
3. If a system administrator adds an EULA, there should only be one active EULA.

4. If a system administrator updates our EULA, only the updated EULA should be displayed
5. If a system administrator deletes the EULA, there should be no EULA displayed.

3.1.3.2. Fail

1. A user or administrator inputs the wrong information when registering, such as putting in the wrong password.
2. When creating an account, user or administrator inputs the correct data and an account isn't created.
3. If a user or administrator inputs incorrect data, such as an already used username, an account is still created.
4. An administrator is able to create another admin account.
5. If a user agrees to the EULA, they are unable to access our system.
6. If a user does not agree to our EULA, they are able to access our system.
7. A system administrator is unable to add, update, or delete our EULA.
8. A normal administrator is able to add, update, or delete our EULA.
9. If there is already an active EULA, another EULA is still able to be added, allowing multiple active EULAs.
10. If the connection drops or server goes down before an account is finished being created, then the account is not created.
11. If the connection drops or server goes down before the EULA is finished being changed, then the EULA is not changed.

3.2. User Management

3.2.1. Functional

3.2.1.1. Enable User Account

Description: A requirement that enables user accounts that were previously disabled.

Business Rules:

1. Disabled user accounts can only be activated by administrators.
2. An administrator will be able to enable multiple accounts at a time.
3. An administrator cannot choose to enable an already active account.
4. Disabled administrator accounts can only be activated by system administrators.
5. Regular administrators are unable to enable another administrator account.

3.2.1.2. Disable User Account

Description: A requirement that disables user accounts by restricting access to the system until it is enabled.

Business Rules:

1. A normal user account can only be disabled by an administrator.
2. Multiple accounts can be disabled at a time.
3. An administrator cannot choose to disable an already inactive account.
4. Administrator accounts can only be disabled by system administrators.
5. A regular administrator account will not be allowed to disable another administrator account.

6. If a user account is disabled, a user will be notified that their account has been disabled, and they are denied access to our system when they try to login.

3.2.1.3. User Delete Account

Description: A user will be able to have their account deleted.

Business Rules:

1. At any point in time, users will be able to request the deletion of their account.
2. When a user account is deleted, all personally identifiable information associated with that account will also be deleted.

3.2.1.4. Administrator Delete Account

Description: A regular user account can be deleted by an administrator.

Business Rules:

1. At any point, an administrator can delete a regular user account.
2. All personally identifiable information related to an account that is deleted will also be deleted at the same time.
3. An administrator account cannot be deleted by another administrator.
4. The ability to delete an administrator account will be limited to system administrators only.
5. Multiple accounts can be deleted at a time.

3.2.1.5. Administrator UAC Configuration

Description: Administrators will be able to modify the rights of what users are able to access.

Business Rules:

1. The UAC for regular users can be changed by administrators.

2. Administrators are unable to modify the UAC for other administrators.
3. The ability to change the UAC of an administrator will be restricted to system administrators only.

3.2.2. Non Functional

1. An account is enabled or disabled in our system less than 4 seconds.
2. It should take less than 4 seconds for an account to be deleted from our system.
3. Updating UAC rights in our system takes less than 4 seconds.
4. Disabling, enabling, and deleting an account should be clear and simple to understand such that 95% of administrators can perform these operations without assistance.

3.2.3. Pass/Fail Scenarios

3.2.3.1. Pass

1. An administrator is able to enable multiple disabled user accounts.
2. An administrator is able to disable multiple enabled user accounts.
3. If a user requests to delete their account or an administrator chooses to delete an account, all information related to that account is also deleted at the same time.
4. Administrators are able to modify what a regular user can access at anytime.
5. A system administrator is able to enable, disable, delete or modify the UAC of an administrator.

3.2.3.2. Fail

1. An administrator enables, disables, deletes, or modifies the UAC of the wrong account.
2. A user accidentally requests for their account to be deleted.

3. An administrator can choose to enable an already enabled account.
4. An administrator can choose to disable an already disabled account.
5. An administrator is able to enable, disable, delete or modify the UAC another administrator account.
6. An administrator is unable to enable, disable, delete, or modify the UAC of a user account.
7. A system admin is unable to enable, disable, delete, or modify the UAC of an administrator account.
8. If connection drops when an account is being enabled, disabled, deleted, or UAC is being modified, then the respective functionality will not be completed.

3.3. Login/Logout

3.3.1. Functional

3.3.1.1. Login

Description: Users are required to enter their username and password in order to access their account.

Business Rules:

1. In order to access an account, the corresponding username and password must be entered.
2. Users will use their email address as their username once it has been verified.
3. Users can create a password between the range of 12 to 2000 characters when making an account.
4. To ensure the security of passwords, it will not be saved into the database as plaintext.
5. Attempting to login to an account through brute force methods will take at least 50 years.
6. If a user fails to login to their account after 3 times, their account will be locked.
7. In the case of locked accounts, only administrators will have the ability to unlock it.

3.3.1.2. Password Reset

Description: A password can be reset by a user while they are not logged into the system. If the user is logged in, the password can be updated.

Business Rules:

1. To reset a password, users will have to answer 3 security questions in addition to a two factor authentication.

3.3.1.3. Logout

Description: Users may end their session when they are finished with the web app.

Business Rules:

1. Users are considered idle if they stay on the same page or there is no activity between their account or the server for thirty minutes.
2. Idle users will automatically be logged out.
3. The timer for idle activity is reset when the server detects activity on the user's end.

3.3.2. Non Functional

1. The time it takes to authenticate a user when logging in should be less than 2.5 seconds.
2. The time it takes to reset or update the password should be less than 2.5 seconds.
3. The time it takes for the user to log out should be less than 2.5 seconds.

3.3.3. Pass/Fail Scenarios

3.3.3.1. Pass

1. Users can login to their accounts if they have a stable connection to the system and enter the correct username and password are entered.
2. Users can log out if they have a stable connection to the system and are logged in.
3. Users can reset their passwords if they have a stable connection to the system.
4. Users can update their passwords if they have a stable connection to they system and they are logged in.

3.3.3.2. Fail

1. A user inputs the wrong password when trying to login.
2. A user logs out unintentionally.
3. A user inputs the wrong answers to their security questions or forgot the answers to their security questions.
4. Users will not be able to access the system or their accounts if the website is down or if they do not have a stable connection to the system.
5. Users are able to login to their accounts if it is disabled.
6. Users are able to login to their accounts if the incorrect username or password is entered.
7. Users cannot reset their password if they enter the correct email address.

3.4. Error Handling

3.4.1. Functional

3.4.1.1. Client-Side Error Handling

Description: Ability to fix/address errors that may occur when a client is using the web app.

Business Rules:

1. Users will be presented with a clear message detailing the error in the event of server request timeouts, invalid server requests, server error, invalid user input, unauthorized access, and when administrator contact is needed.
2. Exceptions will not cause system failure and will only affect the part of the system with the error.
3. In addition to a message of what the error is, possible solutions will be provided.

3.4.1.2. Server-Side Error Handling

Description: Ability to fix/address errors that may occur in the web app's servers.

Business Rules:

1. In the case that an error with the server occurs during a user's session, they will be presented with a clear message detailing the error in the event of invalid requests, server errors, unauthorized access, and when administrator contact is needed.
2. Exceptions will not cause system failure if it is not a critical error and will only affect the part of the system with the error.

3.4.2. Non Functional

1. System must be able to correctly identify the error 100% of the time.

3.4.3. Pass/Fail Scenarios

3.4.3.1. Pass

1. When an error occurs on the user's end, a message occurs that correctly identifies the error and provides possible solutions.
2. When an error occurs on the server, the error will be correctly identified/addressed.

3.4.3.2. Fail

1. User closes error message on accident without reading it.
2. Errors are ignored.
3. A message does not appear if an error occurs.
4. The message on the user's end does not include details of the error or possible solutions.
5. The system crashes if a noncritical error occurs.

3.5. Data Store Access

3.5.1. Functional

3.5.1.1. Create

Description: Functionality to add new records to be stored into the data store system of the web app.

Business Rules:

1. Duplicate entries will not be allowed in the system such as users with the same username.
2. The system will not store new records once space has been capped which is around 250 gigabytes.
3. If the web app fails to load the next action, activity will return to its previous state unless the system states otherwise.

3.5.1.2. Read

Description: Functionality to read data from the data store system.

Business Rules:

1. A response will be sent out to the user if the desired records are not found within the system.
2. The system has a reading limitation depending on the machine technical limitations.
3. If the web app fails to load the next action, activity will return to its previous state unless the system states otherwise.

3.5.1.3. Update

Description: Functionality to update existing records stored in the data store.

Business Rules:

1. A response will be sent out to the user if the desired records to update are not found in the data system.
2. If the web app fails to load the next action, activity will return to its previous state unless the system states otherwise.

3.5.1.4. Delete

Description: Functionality to delete existing records from the data store..

Business Rules:

1. A response will be sent out to the user if the desired records to delete are not found in the data system.
2. If the web app fails to load the next action, activity will return to its previous state unless the system states otherwise.

3.5.1.5. Data Restriction

Description: Controls the amount of access a data access layer has by restricting data access to specific layers.

Business Rules:

1. Data access layer will not request or retrieve data for specific scenarios if the data is not available.

3.5.2. Non Functional

1. Time it takes to update the create, read, update, and delete data should take less than 3 seconds.
2. Data should be retrieved in less than 3 seconds.
3. Time it takes to access create, read, update, and delete data should take less than 3 seconds.

3.5.3. Pass/Fail Scenarios

3.5.3.1. Pass

1. A record will be successfully created if there is space in the data system and there is a stable connection with the website.
2. A record will be successfully read if the selected record can be retrieved from the server.
3. A record will be successfully updated if the selected record can be retrieved from the server.

4. A record will be successfully deleted if the selected record can be retrieved from the server.

3.5.3.2. Fail

1. A record is created, updated, or deleted unintentionally.
2. Data Store Access will fail if the data system is fully capped.
3. Data Store Access will fail if the website is down.
4. Data Store Access will fail if there is no internet connection.
5. Data Store Access will fail if a certain entry is not in the system for read, update, and delete.
6. Data Store Access will fail if the entry logs are left empty.

3.6. User Access Control

3.6.1. Functional

3.6.1.1. Restrict Access/Grant Access

Description: Requirements that restrict and grant access to certain users from performing certain tasks.

Business Rules:

1. The user must be of legal age in the United States in order to use this web-app otherwise they are unable to join.
2. In order for UAC to be validated, a user must be signed in properly.
3. Users who don't have an account are unable to access the system. To inform the unauthorized users the following messages will appear depending on the error request:
    a. A UI message will appear stating the appropriate error and will redirect to the correct page.
    b. A server request message will appear to notify the client of the specific error.
4. User should be able to configure their personal data they used to sign up, game settings, and global settings they have access to.
5. Users can only view, execute, or perform certain tasks to any functionality, data, or content that they have access to.

3.6.2. Non Functional

1. Time it takes for the data to update should be less than 3 seconds.
2. Time it takes for error message to display to unauthorized users should be less than 3 seconds.
3. Time it takes to validate the user for UAC should be less than 3 seconds.

4. Accuracy of displaying error message in the page should be at the center of the page.
5. Time it takes for redirect after error message to occur should be less than 3 seconds.

3.6.3. Pass/Fail Scenarios

3.6.3.1. Pass

1. UAC will pass if the user is authorized, if the data store system isn't capped, and there is a stable connection with the website.
2. UAC will pass if the user is the legal age in the United States.
3. UAC will pass if they signed in to the web-app properly.

3.6.3.2. Fail

1. User Access Control will fail if a user perform some task that they are not authorized to.
2. UAC will fail if there is no stable connection to the internet.
3. UAC will fail if the website is down.
4. UAC will fail if the user already have the granted accesses.

3.7. Logging/Archiving

3.7.1. Functional

3.7.1.1. Error Logging

Description: Requirement that stores a list of errors that the web app has encountered.

Business Rules:

1. When there are at least 100 failed error logs, the system administrator will be notified of the problems.
2. For the error logs to be deleted from the system, the system administrator must delete them.
3. Exceptions that will be recorded into the server from users are the date/time error, error message, incorrect line of code, user affected by the error, and failed user requests.

3.7.1.2. Telemetry

Description: The process of recording specific readings or statistics into a storage type such as database.

Business Rules:

1. If a telemetry receives at least 100 failed telemetry logs, the system administrator will be notified of the issue.
2. Telemetry data that will be recorded are the date/time of user login, date/time of user logout, date/time of user page visit, date/time of user functionality execution, current IP address of logged in user at a specific time, and location of the user logged in at the specific time

3.7.1.3. Malicious Attacks Logging

Description: A requirement that allows requests to be recorded if it means a denial of service attack pattern.

Business Rules:

1. Any requests that follow a suspicious pattern will be logged as denial of service (DOS) attacks.

3.7.1.4. Log Archiving

Description: A requirement that states how all logs should be archived.

Business Rules:

1. Any logs that are older than 30 days, are backed up while any of the logs that are older than 2 years will be deleted from the system. Before the logs are deleted from the system, logs will be backed up and kept of the system for five years before they are deleted as well.
2. For security reasons, if it fails to archive, it will try again in 2 hours.
3. If an archive fails 3 times in its 2 hour interval, the system administrator will be notified of its occurrence.

3.7.1.5. User Data Privacy

Description: A requirement that notifies users to decide if they agree to potential personal data being recorded or prevent certain data from being recorded upon request.

Business Rules:

1. Any information that is recorded must be notified and consented by the user.
2. Any type of information collected from the user must also be able to be viewed by the user.
3. Users can reject the collection of telemetry related data.
4. For security reasons, all of the users data will be deleted from the system upon request if a user deletes their account.

3.7.2. Non Functional

1. Error Logging should be stored in a database in less than 3 seconds after it finds an error.
2. Accuracy of data being logged should be 100%.

3.7.3. Pass/Fail Scenarios

3.7.3.1. Pass

1. If any error or telemetry data is found it will be stored in the server.
2. Personal data will be recorded if consented by user.

3.7.3.2. Fail

1. Error logs, telemetry logs, and malicious attack logs aren't recorded.
2. Logs aren't deleted when they are supposed to be.
3. A user isn't notified about information that is being logged about them.
4. If the server is offline, exceptions will not be recorded.
5. If the server is offline, number of logs will not be able to be calculated. This means that the system administrator will not be able to be notified of any failed errors or failed telemetry. Users will also not be notified of data recorded by the system.
6. If under security threats, any data will not be logged onto the server.

3.8. Usage Analysis Dashboard

3.8.1. Functional

3.8.1.1. Bar Charts

Description: Certain data should be displayed to the administrator or system administrator in bar charts.

Business Rules:

1. Data should be a comparison of the average successful login per month vs total registered users, average session duration per month and failed vs successful login attempts along with the maximum and minimum amounts. Each of the 3 comparisons would have their own measurement in their respective bar charts.
2. Other data that will be displayed in bar chart formats are the top 5 average time spent per page of system and top 5 most used feature in system.

3.8.1.2. Line Charts

Description: Certain data should be displayed to the administrator or system administrator in line charts.

Business Rules:

1. Data should include a timeline of the average session duration per month and the number of users logged in over a span of 6 months. These two data comparisons would be displayed in their own respective line charts.

3.8.2. Non Functional

1. Accuracy of data collected should be at least around 100%.

3.8.3. Pass/Fail Scenarios

3.8.3.1. Pass

1. If server is online, data will be accessed in order to display bar or line charts that display accurate and desired data.

3.8.3.2. Fail

1. If server is not working, data will not be accessed and graphs won't be displayed.
2. If server is online and data is requested, graphs will not be displayed.
3. Charts display out of date or inaccurate data.
4. Data is accurate, but charts do not display the desired data or present it inaccurately.

3.9. Documentation

3.9.1. Functional

3.9.1.1. Developer Docs

Description: Displays information that is helpful for software developers such as documentation on how the code works.

Business Rules:

1. Developer documents are geared towards software developers.
2. Authentication isn't required in order to access the document

3.9.1.2. User Manual

Description: Explains how the web application is used.

Business Rules:

1. A user manual is geared towards normal users .
2. Authentication isn't required in order to access the document.
3. A user manual can only be updated by the system administrator.
4. User Manuals should be as descriptive as possible so it can be valuable resource for users.

3.9.1.3. FAQ

Description: Resolves the most asked questions that are usually asked by the user of the web application.

Business Rules:

1. A FAQ document is geared towards normal users.
2. Authentication isn't required in order to access the document.
3. A FAQ can only be updated by the system administrator.

3.9.2. Pass/Fail Scenarios

3.9.2.1. Pass

1. If a software developer can locate the information they need in the developer documents, then it is successful.

2. If a user can find the answers they need in the FAQ and User Manual, then it is a pass.
3. Users and Software developers are able to access their respective documents if stored in the server.

3.9.2.2. Fail

1. The Developer Docs, FAQ, and User Manual fail if they can not be understood by their target audience.
2. The Developer Docs, FAQ, and User Manual fail if they do not accurately explain what they are supposed to.
3. A developer is unable find the Developer Docs.
4. A user can’t find the FAQ or User Manual.
5. If servers are offline, users will not be able to access FAQ and User Manual.
6. Documentation fails if documents have to be authenticated to be accessed.
7. Documentation fails if the system administrator doesn’t have access to edit the FAQ and User Manual.

4. Application Feature Requirements

4.1. Chat Room

4.1.1. Functional

4.1.1.1. Debate Room

Description: Chat where the debate takes place.

Business Rules:

1. Users will only be able to type into the debate if it is their turn to speak to regulate the flow of the debate.

4.1.1.2. Team Room

Description: Allows teams to have a separate chat room consisting of the team members where they can collaborate.

Business Rules:

1. Only team members can see and participate in the Team Room.

4.1.1.3. Leave Room

Description: Allows users to leave the chat room at any point after the debate starts.

Business Rules:

1. If a judge or the last member of one side leaves the game, the game will end, and the rooms will be closed.
2. If a user leaves a team of more than one person, debate turns will be modified depending on the remaining members.

4.1.2. Non Functional

1. Messages sent through the debate room and team room should be received in less than 2 seconds.
2. The accuracy timer of each phases in the debate should be 100%.

4.1.3. Pass/Fail Scenarios

4.1.3.1. Pass

1. If it is their turn, user is able to chat in the debate room.

2. If users are on the same team, they are able to chat and view conversations in the team room.
3. If users want to leave chat room, they are able to.
4. Game ends after the last user in the chat room leaves.
5. Chat room closes after the game is over.
6. Each user will receive other users' messages in less than 2 seconds.

4.1.3.2. Fail

1. A user unintentionally leaves the room.
2. A user sends a message they did not mean to send in debate room or team room.
3. If it is not their turn, user is able to chat in a debate room.
4. Opposing teams are able to see or chat in the other team's team room.
5. If a user leaves, they are able to re-enter the same chat room.
6. If game ends, timer continues to run.
7. Game continues after all users leave the chat room.
8. Messages do not send within chat rooms.
9. Timer is inaccurate by being ahead or behind.

4.2. Global Setting

4.2.1. Functional

4.2.1.1. Judge Limit

Description: Allows for the host of the debate to limit how many judges are going to be used.

Business Rules:

1. The host of the room will be able to choose to between one to three judges as the limit.

4.2.1.2. Member Limit

Description: Allows for the host of the debate to limit how many people can be on each side of the debate.

Business Rules:

1. A host will have to have at least one person on each side when choosing how many people can be on each side.

4.2.1.3. Spectator Limit

Description: Allows for the host to limit how many spectators can watch the debate in the room.

Business Rules:

1. A host can only allow a maximum of ten spectators to watch the debate, though they can limit it to a smaller number if they desire.

4.2.1.4. Time Limit

Description: Allows for the host of the debate to limit how long the debate will be.

Business Rules:

1. The host can change the time limit of the debate from a minimum of 18 minutes to a maximum of 35 minutes.

4.2.2. Non Functional

1. After the host chooses their configurations, the settings will be updated in less than three seconds.
2. The navigation should be accessible and easy to understand for the user such that 95% of users are able to change settings without assistance.

4.2.3. Pass/Fail Scenarios

4.2.3.1. Pass

1. If host created the room, they will be able to change judge, member, spectator and time limit.
2. If successful, changes will be saved so it can be used in the debate.

4.2.3.2. Fail

1. If server is down, changes won't be able to be saved for the debate.
2. If user's rights are disabled, changes won't be accepted.
3. If user's rights are enabled, changes won't be accepted.
4. If users can surpass the limit of each setting, then it fails.
5. If the time limit ends early by a 2 seconds or late it fails.
6. Host sets the wrong judge, member, spectator, or time limit.

4.3. Game Role Functionality

4.3.1. Functional

4.3.1.1. Assign Role

Description: Players are only allowed to choose the following roles in the game: team1 (proponent for question), team 2 (opponent against question), judge, and spectator after the waiting room.

Business Rules:

1. If the debate doesn't have the maximum amount of debaters allowed, the debating phases will automatically be assigned to the next available player in their respective side.
2. Players are not allowed to switch roles once the game has started.

4.3.1.2. Judge

Description: The judge will decide the winner of the debate.

Business Rules:

1. The judge is only allowed to see the debate chat and does not have access to the team chat.
2. If the judge does not decide on a winner, the result will display as a tie.
3. The maximum amount of judges in a game will be three.

4.3.1.3. Debater

Description: The debater will participate the in the game chat.

Business Rules:

1. Debaters will have a team chat for them to communicate with themselves.
2. There needs to be at least one debater in each side in order to start the game.
3. The maximum amount of debaters will be three per team.

4. Debater are only allowed to respond in the game chat in their own respective phases.
5. Debaters are not allowed to swap responsibilities once the game has started.
6. If the debater doesn’t give a response within the given timer, their turn will be skipped.

4.3.1.4. Spectator

Description: The spectator can join a game to watch the debate.

Business Rules:

1. The maximum amount of spectators in one game will be between five to ten people.
2. Spectators can only watch the debate and will not be able to participate.

4.3.2. Non Functional

1. Accuracy of the timer for the judge to decide the winner should not surpass 1 second after the time limit.
2. Accuracy of the timer for the debater to submit their response should surpass 1 second after the time limit.
3. The transition for the the debater to switch between the team and game chat should be less than one second.
4. The time it takes for a spectator to join an ongoing game should be 3 seconds.
5. The time it takes for the decision to be sent to everyone should be 3 seconds.

4.3.3. Pass/Fail Scenarios

4.3.3.1. Pass

1. If there is at least one debater on both teams and at least one judge, game role functionality will pass.

2. If the user successfully assigned to the role of their choice, then game role functionality will pass.

4.3.3.2. Fail

1. If there is no debater in both side and at least one judge, a message will be displayed notifying user that they need more players.
2. If connection is dropped when selecting a role, the role will not be selected.
3. Spectator will fail if the user joins a game that has been ended for 10 seconds.

4.4. Waiting Room

4.4.1. Functional

4.4.1.1. Start Game

Description: The host will have the option to start the debate.

Business Rules:

1. The host can start the game early if the minimum number of players are in the waiting room.

4.4.1.2. Leave Room

Description: Users will be able to leave the waiting room.

Business Rules:

1. If the host of the room leaves, the waiting room will be closed and all other users will be kicked out.

4.4.1.3. Room Closure

Description: The host will have the ability to close the room kick out all other users.

Business Rules:

1. The waiting room will be closed if the minimum number of players are not in the room by fifteen minutes.

4.4.2. Non Functional

1. The time it take to transition from the waiting room to the game should be less than three seconds.
2. The accuracy of the time limit before the waiting room closes should be 100%.

4.4.3. Pass/Fail Scenario

4.4.3.1. Pass

1. Hosts are able to create a waiting room that other users can join.
2. Users can leave the waiting room at anytime.

3. The host can close the room and other users in the room will be kicked out.
4. The host starts the game early as long as the minimum number of players is met.

4.4.3.2. Fail

1. A waiting room can’t be created.
2. If the host leaves, the room is still open to the other players.
3. The waiting room is still open after fifteen minutes.
4. Users can’t leave the waiting room.
5. The host accidentally starts the game early.
6. The host accidentally leaves or closes the room.
7. A user accidentally leaves the room.

4.5. Matchmaking

4.5.1. Functional

4.5.1.1. Finding a Room

Description: A user will be matched to a random open waiting room.

Business Rules:

1. A user cannot be matched to a room that is already full or to one that does not exist.
2. Users can only try and join one room at a time.
3. If users are already matched into a room, they cannot find another until after they leave the existing room.
4. If finding a room takes longer than 5 minutes, then the user will be informed that they were unable to find a match and be returned to the home page.

4.5.1.2. Creating a Room

Description: A user can create a waiting room so that other users will be able to join their game.

Business Rules:

1. Users are only allowed create one room at a time.
2. If a user is already in a room, they cannot create a new one until they have left the room that they are in.

4.5.1.3. Choose Sides

Description: Users will be able to choose the side of the debate that they want to be on.

Business Rules:

1. Users can only choose to be on one side of the debate.
2. If one side of the debate is full, users will not able to join that side and must join the opposite one.

4.5.1.4. Spectator Search for Active Rooms

Description: Users will be able to spectate ongoing debates by searching for them.

Business Rules:

1. Users can only spectate one debate at a time.
2. A user cannot spectate a debate if they are in a debate.
3. There will be a maximum of ten users that can spectate a debate.

4.5.2. Non Functional

1. Accuracy of the timer to get matched to a game should be 100%.
2. Rooms should be created within five seconds.

4.5.3. Pass/Fail Scenarios

4.5.3.1. Pass

1. If a user chooses to find a room, they are matched to an open waiting room within 5 minutes.
2. If a user chooses to create a room, then a waiting room is created allowing others to join.
3. If a user clicks on an open side, then they will be added to that side.
4. If a user chooses to spectate, then they will be able to select an open room to join and be allowed to spectate.

4.5.3.2. Fail

1. If a user chooses to find a room, they are unable to be matched to an open room within 5 minutes.
2. If a user chooses to create a room, a waiting room is unable to be created or other users are unable to join the room that was created.
3. If a user chooses an open side, they are unable to join it.
4. If a side is full, a user is still able to join it.

5. If a user chooses to spectate, they are not shown the currently ongoing debates.
6. If a user chooses to spectate, they are unable to join an open room or are able to join a room that is full.
7. If connection is dropped while trying to join a game, then they will be unable to connect.
8. A user accidentally finds a room, creates a room, or chooses to spectate.
9. A user accidentally chooses an undesired side in a debate.

4.6. Question Management/Assignment

4.6.1. Functional

4.6.1.1. Add Questions

Description: New questions can be added to the database.

Business Rules:

1. Questions that are going to be added must also include two sides that users will be able to choose from.
2. When adding questions, 1-10 questions can be added at a time.
3. Regular user accounts are unable to add questions.
4. Only administrator accounts can add questions.

4.6.1.2. Question Assignment

Description: The questions stored in our database will be randomly assigned to created debates.

Business Rules:

1. Only one question can be assigned to a debate.
2. A question will be assigned after the host starts the game from the waiting room and roles have been assigned.

4.6.2. Non Functional

1. It should take less than 2.5 seconds for a random question to be assigned to a debate.
2. It should take the database less than three seconds seconds to update when adding a new question.

4.6.3. Pass/Fail Scenarios

4.6.3.1. Pass

1. If an administrator chooses to add questions with the correct fields to the database, then those questions will be added.
2. When a game starts and roles have been assigned, a question will be assigned.

4.6.3.2. Fail

1. An administrator tries to add questions with the correct fields to the database but the questions are not added.
2. The administrator is able to add more than 10 questions to the database at one time.
3. A question is not assigned or it is not assigned in less than 2.5 seconds.
4. If connection drops when a question is being added, then the questions will not be added.
5. If connection drops when a question is being assigned, then the question will not be assigned.
6. An administrator adds a bad or incomplete question.

5. Glossary/Reference

Term	**Description**
EULA	End User License Agreement
FAQ	Frequently Asked Questions
Functional Requirements	Describes what the feature does
IP	Internet Protocol
Non Functional Requirements	Describes how feature works
Telemetry	Simultaneous transmission and recording of data
UAC	User Access Control
UI	User Interface