**Whatever our idea name is**

# **Business Requirement Design**

**Hello World**

**November 18, 2020**

Team Leader: Matt Caponi 011161928

Ian Macabulos 016401240

Jakub Koziol 016523856

Shaan Shariff 015741750

Wonsuk Seo 018660874

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 11/16/20 | <0.1> | Started Outline | Jakub Koziol, Matthew Capone, Shaan Shariff, Ian Macabulos, Wonsuk Seo |
| 11/19/20 | <0.2> | Insert information | Jakub Koziol, Matthew Capone, Shaan Shariff, Ian Macabulos, Wonsuk Seo |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## **Executive Summary**

## **Project Description**

## **Project Scope**

In Scope

Out of Scope

## **Current Process**

## **Core Features**

### **User Management**

* + 1. View All Users
* **Functional Requirements**
  + Admin should be able to view a list of all users along with the following information:
    - Name
    - Email
    - Username
    - Password(?)
    - Permissions
    - Roles
    - Account Status
  + Admin should have the ability to delete, modify, or disable/enable users from this list.
    - Scenario 1
      * Success
        + Successful if the admin can view all users and their relevant information.
      * Failure
        + Unsuccessful if the admin cannot view all users and their relevant information.
    1. User Creation
* **Functional Requirements**
  + User account is created and saved in the account database after the registration process is complete, including the verification of the e-mail.
    - Scenario 1
      * Success
        + If successful, the user account will be created and that user will be able to access the site’s features as well as log out and log back in.
      * Failure
        + If not successful, the attempt to create the user will be aborted. This can happen if the registration process is incomplete, which includes not verifying the e-mail.
  + The user must be unique with a unique user ID and a unique e-mail address to complete registration for the user to be created.
    - Scenario 1
      * Success
        + If successful, the user will be created and no other user can use the same user ID or e-mail address.
      * Failure
        + If not successful, in the event of a user ID or e-mail address already belonging to an existing user, the attempt to create the user will be aborted in the middle of the registration process. Ask the user to enter another email address.
* **Non-Functional Requirements**
  + System Response Time
    - Scenario 1
      * Success
        + System must respond to creating a user within 5 seconds of the registration process being complete.
        + If successful, the user will be created.
      * Failure
        + If the system takes longer than 5 seconds to respond, an admin is notified of the system taking too long.
        + If the system takes longer than 30 seconds to respond, the system will time out, display an error message, and notify an admin.
    1. User Deletion
       1. Admin Deletion
  + **Functional Requirements**
    - Admins will have the ability to delete any user account.
      * Scenario 1
        + Success

Scenario is successful if the selected user account is successfully deleted.

* + - * + Failure

Scenario is a failure if the selected user account still exists after deletion.

* + **Non-Functional Requirements**
* System Response Time
  + Scenario 1
    - Success
      * System must respond to an admin’s action to delete a user within 5 seconds.
      * If successful, the user will be deleted.
    - Failure
      * If the system takes longer than 5 seconds to respond, an admin is notified of the system taking too long.
      * If the system takes longer than 30 seconds to respond, the system will time out, display an error message, and notify an admin.
      1. User-Deletion Request
* **Functional Requirements**
  + A user may delete their account for any reason they choose.
    - Scenario 1
      * Success
        + The user’s account is successfully deleted upon the users’ deletion request.
      * Failure
        + The user’s account is not successfully deleted upon the users’ deletion request.
  + A user may request deletion of their personal data. In this case, all personally identifiable or user identifiable information must be deleted from all servers where it may exist, including:
    - Username
    - Password
    - First Name
    - Last Name
    - Email
    - User ID
    - User Account History
    - User Interactions
  + User posts and messages will not be deleted, however, any PID information associated with those posts/messages must be deleted.
    - Scenario 1
      * Success
        + All PID information about the user or user-identifiable information is successfully deleted from all servers where it may exist.
      * Failure
        + All PID information about the user or user-identifiable information is not successfully deleted from all servers where it may exist.
* **Non-Functional Requirements**
  + System Response Time
    - Scenario 1
      * Success
        + System must respond to a user’s request for user deletion within 5 seconds.
        + If successful, the user request will be sent to the admins so the admins can delete the user.
      * Failure
        + If the system takes longer than 5 seconds to respond, an admin is notified of the system taking too long.
        + If the system takes longer than 30 seconds to respond, the system will time out, display an error message, and notify an admin.
    1. Enable/Disable a User
       1. Admin Enable
* **Functional Requirements**
  + Admin can enable a disabled user account upon request of the user.
    - Scenario 1
      * Success
        + If successful, the disabled user account will be enabled and the user will gain access to the site’s features.
      * Failure
        + If not successful, the disabled user account will remain disabled.
* **Non-Functional Requirements**
  + System Response Time
    - Scenario 1
      * Success
        + System must respond to an admin’s action to enable a disabled user within 5 seconds.
        + If successful, the admin will enable the disabled user.
      * Failure
        + If the system takes longer than 5 seconds to respond, an admin is notified of the system taking too long.
        + If the system takes longer than 30 seconds to respond, the system will time out, display an error message, and notify an admin.
      1. User Enable
* **Functional Requirements**
  + Users can choose to enable their account after previously having chosen to disable it.
    - Scenario 1
      * Success
        + The user account will be enabled and be able to re-access the site’s feature.
      * Failure
        + The user account will remain disabled.
* **Non-Functional Requirements**
  + System Response Time
    - Scenario 1
      * Success
        + System must respond to a user’s request to enable the user account within 5 seconds.
        + If successful, the system will enable the disabled user account.
      * Failure
        + If the system takes longer than 5 seconds to respond, an admin is notified of the system taking too long.
        + If the system takes longer than 30 seconds to respond, the system will time out, display an error message, and notify an admin.
      1. Admin Disable
* **Functional Requirements**
  + An admin can disable a user account for the purposes of temporary suspension.
    - Scenario 1
      * Success
        + The user account has been successfully disabled and the user can no longer access the account.
      * Fail
        + The user account has not been successfully disabled and the user can still access the account.
* **Non-Functional Requirements**
  + System Response Time
    - Scenario 1
      * Success
        + System must respond to an admin’s action to disable a user account within 5 seconds.
        + If successful, the user account will be disabled.
      * Failure
        + If the system takes longer than 5 seconds to respond, an admin is notified of the system taking too long.
        + If the system takes longer than 30 seconds to respond, the system will time out, display an error message, and notify an admin.
      1. User Disable
* **Functional Requirements**
  + A user can decide to disable their own account if they wish to suspend activity but would like their account to remain for future activation.
    - Scenario 1
      * Success
        + The user successfully disables their account and can no longer access it without re-enabling.
      * Fail
        + The user was not successful in disabling their account and can still access it normally.
* **Non-Functional Requirements**
  + System Response Time
    - Scenario 1
      * Success
        + System must respond to a user’s request to disable their user account within 5 seconds.
        + If successful, the user account will be disabled.
      * Failure
        + If the system takes longer than 5 seconds to respond, an admin is notified of the system taking too long.
        + If the system takes longer than 30 seconds to respond, the system will time out, display an error message, and notify an admin.
    1. Modify User Account
       1. Change User Access
* **Functional Requirements**
  + An admin can change a user’s access to either:
    - Developer
    - Admin
    - Regular User
    - Scenario 1
      * Success
        + User’s role is successfully changed.
        + User has access to everything they should have access to for their role.
      * Fail
        + User’s role is not successfully changed.
        + User’s role is changed but they do not have access to what they should have access to for their role.
* **Non-Functional Requirements**
  + System Response Time
    - Scenario 1
      * Success
        + System must respond to the role change within 5 seconds.
        + If successful, the user account’s role will be changed.
      * Failure
        + If the system takes longer than 5 seconds to respond, an admin is notified of the system taking too long.
        + If the system takes longer than 30 seconds to respond, the system will time out, display an error message, and notify an admin.
    1. Update User Account Info
* **Functional Requirements**
  + User change username
    - Scenario 1
      * Success
        + Successful if the user’s username is successfully and accurately changed after attempt.
      * Fail
        + Not successful if the user’s username is not successfully or accurately changed after an attempt.
  + User change password
    - Scenario 1
      * Success
        + Successful if the user’s password is successfully and accurately changed after attempt.
      * Fail
        + Not successful if the user’s password is not successfully or accurately changed after attempt.
  + User change email
    - Scenario 1
      * Success
        + Successful if the user’s email is successfully and accurately changed after attempt.
      * Fail
        + Not successful if the user’s email is not successfully or accurately changed after attempt.
  + Admin change user password
    - Scenario 1
      * Success
        + Successful if the user’s password is successfully and accurately changed after attempt.
      * Fail
        + Not successful if the user’s password is not successfully or accurately changed after attempt.
* **Non-Functional Requirements**
  + System Response Time
    - Scenario 1
      * Success
        + System must respond to any user account change within 5 seconds.
        + If successful, the user account’s change will take place.
      * Failure
        + If the system takes longer than 5 seconds to respond, an admin is notified of the system taking too long.
        + If the system takes longer than 30 seconds to respond, the system will time out, display an error message, and notify an admin.

### **Logging**

### **General Logging Requirements (High)**

### **Functional Requirements**

* + - Logs every transaction done by the user and the system. Each log happens synchronously along with the activity.
      * Success
        + If successful, the system will log the data after the activity has been placed.
      * Failure
        + If not successful, the attempt to log will be aborted.
    - All logs should include the following components:
      * Date/Timestamp
        + Date
        + Time
      * Log Level
        + Trace
        + Debug
        + Information
        + Warning
        + Error
        + Critical
      * Who is calling the log
      * Message
        + Success

If successful, the log saved will have all of the given components.

* + - * + Failure

If not successful, the log saved will have only the components the system could save, or none at all.

### **Non-Functional Requirements**

* + System Response Time
    - Scenario 1
      * Success
        + System must successfully log data within 5 seconds after every time a log needs to be produced.
        + If successfully logged, the log and its data is saved accurately.
      * Fail
        + System attempts to log longer than 5 seconds.
        + If not successful, abort the attempt of a log.
  + Log Accuracy
    - Scenario 1
      * Success
        + All logs contain accurate log information in accordance with the specified log info for that log type.
      * Fail
        + Some or all of the information in any given log is not accurate with the log info specified for that log type.

### **Registration Logging**

* + **Log Info**
    - IP Address
  + **Functional Requirements**
    - Logs whenever a successful user registration is made
      * Log Info
        + User id assigned.
      * Success
        + A log is successfully produced when the user registers for an account
      * Fail
        + A log is not created when the user successfully registers an account.
    - Logs whenever a failed user registration is made.
      * Success
        + A log is successfully produced when the user fails or commits an error during registration
      * Fail
        + A log is not produced when the user fails or commits an error during registration.
    - A log is produced if the user enters information with illegal characters.
      * Success
        + A log is successfully produced each time the user enters information with illegal characters.
      * Failure
        + A log is not successfully produced each time the user enters incorrectly formatted input into either or both text fields.
    - A log is produced if the user enters an email that is not in the correct email format.
      * Scenario 1
        + Success

A log is successfully produced each time the user enters an email that is not in the correct email format.

* + - * + Fail

A log is not successfully produced each time the user enters an email that is not in the correct email format.

* + - A log is produced if the user enters information that exceeds or fails to meet minimum and maximum string length.
      * Success
        + A log is successfully produced if the user enters information that exceeds or fails to meet minimum and maximum string length.
      * Failure
        + A log is not successfully produced if the user enters information that exceeds or fails to meet minimum and maximum string length.
    - A log is produced if the user attempts to register with information that belongs to an already existing account.
      * Success
        + A log is successfully produced if the user attempts to register with information that belongs to an already existing account.
      * Failure
        + A log is not successfully produced if the user attempts to register with information that belongs to an already existing account.
    - A log is produced if the user requests another email to be sent.
      * Success
        + A log is successfully produced when the user asks for another email to be sent.
      * Failure
        + A log is not successfully produced when the user asks for another email to be sent.
    - A log is produced when an e-mail is sent to the user.
      * Success
        + A log is successfully produced when an e-mail is sent to the user.
      * Failure
        + A log is not produced when an e-mail is sent to the user.
    - A log is produced when a user verifies their e-mail address from the e-mail sent.
      * Success
        + A log is successfully produced when a user verifies their e-mail address from the e-mail sent to them.
      * Failure
        + A log will not be produced when a user verifies their e-mail address from the e-mail sent to them.
    - A log is produced when an email verification expires
      * Success
        + A log is successfully produced when a user verifies their e-mail.
      * Failure
        + A log will not be created when an email verification expires because the user does not verify their e-mail.
  + **Non-Functional Requirements** 
    - System Response Time
      * Scenario 1
        + Success

System must successfully log registration data within 5 seconds after every time a log needs to be produced.

If successfully logged, the registration log and its data is saved accurately.

* + - * + Fail

System attempts to log longer than 5 seconds.

If not successful, abort the attempt of the registration log.

* + - * Scenario 2
        + Success

System must successfully log the instance the e-mail has been sent or verified within 5 seconds.

If successfully logged, the log about the e-mail will be saved accurately.

* + - * + Failure

System attempts to log longer than 5 seconds.

If not successful, abort the attempt of the log involving the e-mail.

### **Login**

* + **Functional Requirements**
    - A log is produced whenever a user logs in.
      * Log info
        + User ID
        + User Type
        + Time
      * Scenario 1
        + Success

A log is successfully produced when the user logs in.

* + - * + Failure

Log is not successfully produced when the user logs in.

* + - A log is produced upon each failed attempt to login.
      * Log info
        + IP Address
        + Time
      * Scenario 1
        + Success

A log is successfully produced each time the user fails to log in.

* + - * + Failure

A log is not successfully produced for each time the user fails to log in.

* + - A log is produced if the user selects the “forgot username” option.
      * Scenario 1
        + Success

A log is A log is successfully produced each time the user selects “forgot username”.

* + - * + Failure

A log is not successfully produced each time the user selects “forgot username”.

* + - A log is produced if the user selects the “forgot password” option.
      * Scenario 1
        + Success

A log is successfully produced each time the user selects “forgot password”.

* + - * + Failure

A log is not successfully produced each time the user selects “forgot password”.

* + - A log is produced if the user enters an incorrect username.
      * Scenario 1
        + Success

A log is successfully produced each time the user enters incorrectly formatted input into either or both text fields.

* + - * + Failure

A log is not successfully produced each time the user enters incorrectly formatted input into either or both text fields.

* + - A log is produced if the user enters an incorrect password.
      * Scenario 1
        + Success

A log is successfully produced each time the user enters an incorrect password.

* + - * + Failure

A log is not successfully produced each time the user enters an incorrect password.

* + - A log is produced if the user enters information for an account that does not exist.
      * Scenario 1
        + Success

A log is successfully produced each time the user enters information for an account that does not exist.

* + - * + Failure

A log is not successfully produced each time the user enters information for an account that does not exist.

* + - A log is produced if the user attempts to log into a disabled or locked account.
      * Scenario 1
        + Success

A log is successfully produced each time the user attempts to log into a disabled or locked account.

* + - * + Failure

A log is not successfully produced each time the user attempts to log into a disabled or locked account.

* + **Non-Functional Requirements** 
    - System Response Time
      * Scenario 1
        + Success

System must successfully log the login data within 5 seconds after every time a log needs to be produced.

If successfully logged, the login log and its data is saved accurately.

* + - * + Fail

System attempts to log longer than 5 seconds.

If not successful, abort the attempt of the login log.

### **User Management Logging**

* + **Functional Requirements**
    - Log Info
      * User ID
      * IP address
    - A log is produced if a user registers and their information is successfully validated and entered into the datastore.
      * Scenario 1
        + Success

A log is successfully produced each time a user registers for an account successfully.

* + - * + Failure

A log is not successfully produced each time a user registers for an account successfully.

* + - A log is produced if a user deletes their account.
      * Scenario 1
        + Success

A log is successfully produced each time a user successfully deletes an account.

* + - * + Failure

A log is not successfully produced each time a user successfully deletes an account.

* + - A log is produced if an admin deletes a user account.
      * Scenario 1
        + Success

A log is successfully produced each time an admin deletes a user account.

* + - * + Failure

A log is not successfully produced each time an admin deletes a user account.

* + - A log is produced if an admin disables a user account.
      * Success
        + A log is successfully produced each time an admin disables a user account.
      * Failure
        + A log is not successfully produced each time an admin disables a user account.
    - A log is produced if an admin enables a user account.
      * Success
        + A log is successfully produced each time an admin enables a user account.
      * Failure
        + A log is not successfully produced each time an admin enables a user account.

* + **Non-Functional Requirements**
    - Log info
      * Time
      * IP address
    - A log is produced If the system takes more then 5 seconds to respond this is considered an error.
      * Scenario 1
        + Success

The login system must respond within 5 seconds

Success occurs when the login system fails to respond in 5 seconds and the error is logged

* + - * + Failure

Failure occurs when the login system does not respond in 5 seconds and the error is not logged

* + - A log is produced if the system takes more than 30 seconds to work the system will time out
      * Scenario 1
        + Success

If the login system takes longer than 30 seconds to respond and the system times out log the error

Success occurs when an log is created if the login system times out

* + - * + Failure

Failure occurs that after a 30 second timeout the login system does not create an error log

### **Security Logging**

* + **Functional Requirements** 
    - Log info
      * IP addresses
    - A log is produced if the DDoS prevention system detects an attempted DDoS attack onto our servers.
      * Scenario 1
        + Success

A log is successfully produced when the system detects a DDos attack.

* + - * + Failure

A log is not successfully produced when the system detects a DDos attack.

* + - A log will be produced when a login attempt fails 5 or more times.
      * Log info
        + User ID
        + Operating System
      * Scenario 1
        + Success

A successful log is produced each time a user fails to login 5 or more times.

* + - * + Failure

A successful log is not produced each time a user fails to login 5 or more times.

* + - A log is produced if there is a login attempt on a temporarily locked account.
      * Scenario 1
        + Success

A Log is successfully produced when login attempts on a locked account are detected.

* + - * + Failure

A Log is not successfully produced when login attempts on a locked account are detected.

* + - A log is produced if a network connection to the system is not secured by an https encryption.
      * Log info
        + Website address
        + Client operating system
      * Scenario 1
        + Success

A log is successfully produced when the system logs network connections that are not encrypted by HTTPS.

* + - * + Failure

A log is not successfully produced when the system logs network connections that are not encrypted by HTTPS.

* + - A log is produced if a dangerous connection is detected going past the firewall
      * Log info
        + Connection type
        + IP address
        + Time
      * Scenario 1
        + Success

When a rouge connection is detected on the firewall block it and log the event

If successful the firewall will log when a rogue connection event is detected at the firewall

* + - * + Failure

Failure occurs when a rogue connection is detected at the firewall but the event is not logged.

* + **Non-Functional Requirements**
    - System Response Time
      * Log info
        + Time
        + IP address
        + Run time
    - Scenario 1
      * Success
        + System must successfully log security data within 5 seconds after every time a log needs to be produced.
        + If successfully logged, the security log and its data is saved accurately.
      * Fail
        + System attempts to log longer than 5 seconds.
        + If not successful, abort the attempt of the security log.

### **Network Logging**

* **Functional Requirements**
  + Log info
    - IP address
    - Page request
    - HTTP status
    - HTTP refer
    - User agent
  + A log is produced when a new user or non user/ new ip address visits the website
    - Scenario1
      * Success
        + A log is created when someone new visits the website for the first time.
      * Fail
        + A log is not created when a new visitor visits our website.
  + A log is produced when someone clicks on a webpage link
    - Scenario1
      * Success
        + A log is successfully created whenever a webpage link is clicked on.
      * Fail
        + A log is not created whenever a webpage link is clicked
* **Non-Functional Requirements**
  + System Response Time
    - Scenario 1
      * Success
        + System must successfully log network data within 5 seconds after every time a log needs to be produced.
        + If successfully logged, the network log and its data is saved accurately.
      * Fail
        + System attempts to log longer than 5 seconds.
        + If not successful, abort the attempt of the network log.

### **Error Handling Logging**

* + **Functional Requirements**
    - Log info
      * Error type
      * Error messages
      * Context
      * Time
    - A log is produced if the system handles an error
      * Scenario 1
        + Success

A log is successfully produced anytime there is an error.

* + - * + Fail

A log is not successfully produced anytime there is an error.

* + **Non-Functional Requirements**
    - System Response Time
      * Scenario 1
        + Success

System must successfully log error data within 5 seconds after every time a log needs to be produced.

If successfully logged, the error log and its data is saved accurately.

* + - * + Fail

System attempts to log longer than 5 seconds.

If not successful, abort the attempt of the error log.

### Intelligent Search Engine

### Traditional Listings

### Traditional Posting Search

### Friend List

### Private Messaging

### Group Pages

### User-Interactions

### reCAPTCHA

### User Profile

### Moderator Controls

### 

* + - Logs user’s contact information, including their current IP address
      * Does not log passwords
      * Success
        + If successful, the user information log will be saved in the database.
      * Failure
        + If not successful, the attempt to log the user information will be aborted.

\*\*\*\*\*\* for Registration features

**General**

* + - **Functional Requirements(user or system does)**
      * Users register by inputting their information into the UI.
        + Scenario 1
        + Success:

Users are able to input their info into the given text boxes.

* + - * + Fail:

Users are not able to type in their information/ The system does not present the user with the registration page.

* + - * Scenario 2
        + Success:

Users are able to register into our user database and are added successfully.

* + - * + Fail:

Users are able to submit their registration form into the system. However, users are not added into the database or their information has been added in incorrectly. (i.e. corresponding information is not stored into their respective categories.)

* + - **Non-Functional Requirements(quality of the system)**

\*\*\*\*\* for log in features

**General**

* + - **Functional Requirements**
      * Users are able to log into the website using their registered username and password.
        + Scenario 1

Success

Users are able to log in and penetrate through the login page and into our website.

Fail

Users are not able to log into our website even if the correct username and password is inputted.

* + - * System gives the user multiple tries to log into the website in case of human error with inputs.
        + Scenario 1

Success

Users are given an error message saying that they inputted the wrong username or password. They are given more chances to log in

Fail

Users are not able to keep trying after 1 unsuccessful log in. They are locked out of the website for some time.

* + - **Non-Functional Requirements**

### **Security\*This should go into feature was writing it wrong will input when we get there**

* + **General**
    - **Functional Requirements** 
      * Network transmissions will be encrypted using forced HTTPS SSL encryptions to ensure the privacy of the data sent
        + Scenario 1

Success

All of the network transmissions will be encrypted using forced HTTPS SSL encryptions to ensure the privacy of the data sent

Success occurs when all data sent over the network is encrypted in force HTTPS SSL

Failure

Failure occurs when there is data sent over the network that does not use forced HTTPS SSL

* + - * Confidential and critical data stored in our datastore will be encrypted with md6 encryption to ensure that all of this data is secure
        + Scenario 1

Success

All of the critical data stored in the datastores will be encrypted with an md5 encryption

Success occurs when all of the critical data in our datastores is encrypted with a md5 encryption

Failure

Failure occurs when the data in our datastores is not encrypted with md5

* + - * If an attempted DDoS attack is detected the DDoS prevention system will activate and force all connection to the site to wait 5 seconds before connecting and blocking out ip address
        + Scenario 1

Success

If a DDoS attack is detected block out the suspected ip address and force all other IP’s to a delay of 5 seconds before connection

If successful when a DDoS attack is detected block out the suspected ip address and force all other IP’s to a delay of 5 seconds before connection

Failure

Failure occurs when the system does not block out all suspected DDoS IP addresses

Failure occurs when the system does not delay all connections by 5 seconds before connecting

* + - * If a suspicious connection is detected to the web server the firewall will block out the connection
        + Scenario 1

Success

When a suspicious ip address attempts to connect to the webserver the firewall will block the connection

If successful when a suspicious connection is detected the connection will be blocked by the firewall

Failure

Failure occurs when a suspicious connection is allowed without the firewall blocking the connection

* + - * If a code repository or code api is used which has had a vulnerability noted notify the system administers once the issue is known
        + Scenario 1

Success

When an imported code library is known to have a vulnerability in it the system will notify that system admin of the issue

If successful when a vulnerable code library is detected the system admin will be notified of the issue

Failure

Failure occurs when a vulnerability is found in one of the external code libraries being used and the system does not notify the system admin of the issue.

* + - * Inside of the application there will be webpages which will be accessible to only approved users. The security system must verify that only allowed users can access these pages.
        + Scenario 1

Success

When an authorized user attempts to access a restricted page they are allowed to access the page, but if an unauthorized users attempts to access the restricted page they will be shown an error

If successful all pages which are confidential will only be accessible by people with access to those pages

Failure

Failure occurs when unauthorized users are able to access restricted pages in the web application

* + - * Since users will be entering confidential information into the application it is important that all this information is securely stored and not accessible from anyone.
        + Scenario 1

Succes

When confidential information is entered into the site, this information will not be extractable by searching through the site cookies

If successful no confidential information will be stored inside of the cookies of the site

Failure

Failure occurs when confidential data is stored within the cookies of the website

* + - * The website has to be coded to prevent SQL injection but you can never be 100% certain that such an attack can occur. The sql server must be verifying that there are no suspicious queries being created and if a suspicious query is created the SQL server must block it.
        + Scenario 1

Success

When a query is created to the SQL server that is suspected to be an SQL injection block the query, if it was indeed a proper query the system admin will have to white list it in the SQL server setting

If successful any suspicious query will be blocked to help prevent SQL injection attacks

Failure

Failure occurs when a suspicious SQL injection query is allowed to run inside of the SQL server

* + - * The web and backend server will be running a security scan that will try and identify any commonly misconfigured systems within the server's configuration
        + Scenario 1

Success

The configuration scanner will run automatically at a set time and scan for commonly misconfigured configurations

If successful the configuration scanner will scan the systems to verify that all systems are configured properly

Failure

Failure occurs when the system does not run automatically at a set time

* + - * + Scenario 2

Success

The configuration scanner will identify configuration issues then notify the system admin of these issue

If successful the configuration scanner will notify the system admin when a misconfigured system is found

Failure

Failure occurs when the system finds a misconfigured system and fails to notify the system admin

Failure occurs when the system scans a misconfigured configuration and does not notice that the configuration is incorrectly implemented.

* + - * To prevent deserialization attacks we must only sterilize mediums that use a primitive data type or use integrity checks to verify that all objects have correct signature and isolate all code that could have the possibility of a deserialization attack.
        + Scenario 1

Success

If possible the sterilization of data will only sterilize a primate data type

If successful the system will only sterilize primitive data types

Failure

Failure occurs when the system must sterilize non primitive data types and the system then become vulnerable to deserialization attacks

* + - * + Scenario 2

Success

If the system must deserialize non primitive data types the system must be isolated from every other system so remote code injection threats are limited.

If successful the system will have all sterilization system isolated from the rest of the application

Failure

Failure occurs when the system needing sterilization is not isolated from the rest of the system, which results in remote code execution vulnerabilities

* + - **Non Functional Requirements** 
      * System response time
        + Scenario 1

Success

For all security features the response times for the system must be 400ms

If successful the response time for the system will be 400ms

Failure

Failure occurs when the system takes more than 5 seconds to function

* + - * + Scenario 2

Success

If the response time for the system takes more than 30 seconds the system will timeout

If the system takes more than 30 seconds to respond the system will time out

Failure

Failure occurs when the system takes more than 30 seconds to respond and the system does not time out after that time

//removed from security

* + - A log is created when someone attempts to login to a location requiring authentication
      * Log Info
        + IP address
        + Operating System
        + Time
        + Page
        + User ID
      * Scenario 1
        + Success

When someone logs into a location requiring higher authentication log the event

Is successful when someone logs into a page requiring higher authentication log the login

* + - * + Failure

Failure occurs when someone logs into a page requiring higher authentication and the login is not logged.