Khan, Faisal

S1828698



Coursework – Stage 1

Secure Software Development

Table of Contents

[1. System Assumptions 3](#_Toc24043834)

[2. Security Requirements 4](#_Toc24043835)

[2.1 Authentication and Authorisation 4](#_Toc24043836)

[2.1 Injection Attacks 4](#_Toc24043837)

[3. System Design 5](#_Toc24043838)

[3.1 Entity Relationship Diagram 6](#_Toc24043839)

[4. Test Plan 7](#_Toc24043840)

[4.1 Registration/Login 7](#_Toc24043841)

[4.2 Creating a Ticket 7](#_Toc24043842)

[4.3 Creating a Comment 8](#_Toc24043843)

[4.4 Database Access 9](#_Toc24043844)

# System Assumptions

1. The users of the application are already registered
2. The user is required to enter a valid combination of a username and password in order to access the application
3. The user’s details will be encrypted for security purposes (e.g. passwords)
4. The user’s details should contain the following: UserID, Username, Password and User Role
5. The application will have unique user privileges for different users (developers, testers and clients), this will be handled via a separate database table
6. Connection to the application will be made secure by using TLS
7. The host server will ensure it includes a firewall to prevent attackers from accessing the application
8. A new session is created when a user logs into the system
9. The sessionID will be encrypted
10. The session will expire after 10 minutes if no user interaction is detected
11. A ticket should be created for every bug that is found
12. Three types of tickets: development, testing and production
13. The ticket will consist of the following information: ticket number, date, timestamp, description of bug or error, name of bug founder and the developer who it will be assigned to. This information will also be encrypted.
14. Tickets will possess a priority value of – low, medium or high
15. An encrypted comment section will also be included for each ticket and should contain a timestamp and the name of the individual who appointed the comment
16. Tickets will have a status as – open, resolved or closed
17. Comments can only be appended to tickets which have a status of open or resolved
18. Closed tickets cannot inhibit comments unless the status is altered to open

# Security Requirements

## Authentication and Authorisation

* The application should only be accessed by authenticated users via a unique username and password. The username and password combination will be stored in a database for all users.
* Passwords will ought to be encrypted as it is crucial for the security of the application. With the threat of a hack/breach of the application, the passwords will remain protected. Password validation should also be incorporated to reduce the use of vulnerable/weak passwords.
* Create specific user privileges with the purpose of limiting the access rights of each user. Developers, testers and clients would all have specific restrictions when using the bug tracking application.
* Using secure connections such as Transport Layer Security(TLS) or Secure Sockets Layer(SSL) ensures the authentication of the application will be validated and data integrity is maintained.
* Two-Factor authentication could also be considered to make the system more secure and eliminating the risk of attackers breaching the system. This can be in the form of a specific code sent via email or mobile number to the user.

## Injection Attacks

* Attackers can use SQL injection to manipulate the database behind the application and with the information gathered, can simply bypass the authentication and authorisation stages. Attackers can then access sensitive information regarding clients and other users. By validating all user input on both the client side and server side, abnormal data will be reduced from entering the system/database. This shall be performed by ensuring the data is: strongly typed, permitted characters, correct syntax etc.
* Encrypting tickets and ticket information will add an extra security feature to discourage attackers from gaining unauthorised access to the application and its contents.
* Comments shall be encrypted as attackers could alter the contents of the comment leading to misguided feedback.
* Filtering characters such as the following (<, >, “, ‘ etc.) can reduce the effects of XSS attacks if the system were to be compromised

# System Design

The following diagram shows the secure design of the web application. The application will contain a firewall between the front-end and the backend.

A screenshot of a cell phone

Description automatically generated

## Entity Relationship Diagram

The following diagram illustrates the database implementation of the application. It also shows the key entities and the relationships between them within the scope of the system.

A picture containing screenshot

Description automatically generated

# Test Plan

Below is a test plan for each crucial part of the bug tracking application. This test plan will then be applied when testing the prototype made.

## Registration/Login

|  |  |  |  |
| --- | --- | --- | --- |
| Test ID | Description | Input | Expected Result |
| 1 | Password | 1234 | Deny |
| 2 | Password | -1234 | Deny |
| 3 | Password | Password | Deny |
| 4 | Password | <src=pass> | Deny |
| 5 | Password | N/A | Deny |
| 6 | Password | Password!23$ | Accept |
| 7 | Username | N/A | Deny |
| 8 | Username | 1234 | Deny |
| 9 | Username | User12@test.com | Accept |

## Creating a Ticket

|  |  |  |  |
| --- | --- | --- | --- |
| Test ID | Description | Input | Expected Result |
| 1 | Date | -06/11/19 | Deny |
| 2 | Date | 19/11/06 | Deny |
| 3 | Date | 06/11/2019 | Accept |
| 4 | Timestamp | -06-11-2019 16:00:00 | Deny |
| 5 | Timestamp | 06/11/2019 16:00:00 | Accept |
| 6 | Description of bug | N/A | Deny |
| 7 | Description of bug | “There is a logic error on line 16” | Accept |
| 8 | Name of founder | N/A | Deny |
| 9 | Name of founder | “User12” | Accept |
| 10 | Assigned to | N/A | Deny |
| 11 | Assigned to | “Developer1” | Accept |
| 12 | Priority Value | N/A | Deny |
| 13 | Priority Value | Important | Deny |
| 14 | Priority Value | Any value from: low, medium or high | Accept |

## Creating a Comment

|  |  |  |  |
| --- | --- | --- | --- |
| Test ID | Description | Input | Expected Result |
| 1 | Comment | N/A | Deny |
| 2 | Comment | “This is a comment” | Accept |
| 3 | Comment Timestamp | -06-11-2019 16:00:00 | Deny |
| 4 | Comment Timestamp | 06/11/2019 16:00:00 | Accept |
| 5 | Comment creator | N/A | Deny |
| 6 | Comment creator | “User12” | Accept |
| 7 | Ticket status | N/A | Deny |
| 8 | Ticket Status | Any value from: open, resolved or closed | Accept |
| 9 | Ticket Status: Open | “This is a comment” | Accept |
| 10 | Ticket Status: Resolved | “This is a comment” | Accept |
| 11 | Ticket Status: Closed | “This is a comment” | Deny |

## Database Access

|  |  |  |  |
| --- | --- | --- | --- |
| Test ID | Description | Input | Expected Result |
| 1 | Encrypted passwords | Viewing password fields | Qwe548495bbjd73lkshjgf |
| 2 | Logging into the application | Incorrect Username  Correct Password | Deny |
| 3 | Logging into the application | Correct Username  Incorrect Password | Deny |
| 4 | Logging into the application | Correct Username  Correct Password | Accept |
| 5 | Encryption of tickets | Viewing tickets | 43i5uhfniuf893r4f98nw |
| 6 | Encryption of comments | Viewing comments | 8237tfb87c73y87fddew |