Faisal

Student ID: S1828698

Secure Software Development

Coursework Stage 2

Table of Contents

[Client 2](#_Toc26135916)

[Server 2](#_Toc26135917)

[Data 2](#_Toc26135918)

[Security Controls 2](#_Toc26135919)

[Authentication Attacks 2](#_Toc26135920)

[Authorisation Attacks 3](#_Toc26135921)

[Injection Attacks 3](#_Toc26135922)

[Testing 4](#_Toc26135923)

# Client

The client side for the bug tracking application was implemented using ASP.NET with the MVC (Model, View and Controller) architectural pattern in conjunction with C# as the programming language. When a new bug ticket is created, appropriate validation is carried out on the client side ensuring fields contain the required type of information. Validation such as checking whether fields contain invalid characters (ex. < > ‘ “ = +) is achieved by using data attributes which are applied on the client and the server.

# Server

ASP.NET supports a variety of relational and non-relational data stores. The server utilised in this solution for the management of data access and retrieval was SQL Server. SQL Server uses a selection of SQL statements which add, update, retrieve and delete queries based on the requirements of the statement. Along with ASP.NET is Entity Framework which allows effortless access to the database using LINQ. Entity Framework translates the LINQ to SQL and executes the commands against the database. In order to maximise workflow, the Code First approach was employed provided by Entity Framework, which uses Code First Migrations to update the database after a model change.

# Data

As mentioned above, the data is stored in SQL Server. To improve data security, sensitive data such as passwords are hashed to reduce the possibility of an attacker obtaining such data. Account lockout is enabled to ensure maximum security of the user’s account, this can be caused by a certain number of invalid attempts at the login stage. Another feature built into the application includes a ValidateAntiForgeryToken which represents an attribute that is used to prevent forgery of a request.

# Security Controls

## Authentication Attacks

Authentication attacks such as brute force and insufficient authentication allows attackers to gain access to a site by either guessing a user’s username and password or due to the lack of proper authentication rules implemented on the site. To prevent this, after a certain amount of login attempts the account will be locked out.

## Authorisation Attacks

Authorisation follows authentication and thus gives the authenticated user their appropriate rights and privileges in the system. These are commonly used in conjunction with each other as both are critical to any system holding data. The bug tracking solution complies with this by containing different user roles. Only administrative users of the system can alter and create tickets.

## Injection Attacks

Injection Attacks such as XSS (Cross-site Scripting) and SQL Injection can be brutal towards systems containing data such as the bug tracking solution. In order to reduce the risk of such attacks, an expression annotation is used for each data entry in order to reject certain characters. Another preventative measure implemented is Anti-Forgery Tokens which generates a hidden form field that is validated when the form is submitted.

# Testing

Below is a test plan for each crucial part of the bug tracking application.

## Registration/Login

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test ID | Description | Input | Expected Result | Screenshot |
| 1 | Password | 1234 | Deny | A screenshot of a cell phone  Description automatically generated |
| 2 | Password | -1234 | Deny | A screenshot of a cell phone  Description automatically generated |
| 3 | Password | Password | Deny | A screenshot of a cell phone  Description automatically generated |
| 4 | Password | <src=pass> | Deny | A screenshot of a cell phone  Description automatically generated |
| 5 | Password | N/A | Deny | A screenshot of a cell phone  Description automatically generated |
| 6 | Password | Password!23$ | Accept | A screenshot of a cell phone  Description automatically generated |
| 7 | Username | N/A | Deny | A screenshot of a cell phone  Description automatically generated |
| 8 | Username | 1234 | Deny | A screenshot of a cell phone  Description automatically generated |
| 9 | Username | Test@tesing.com | Accept | A screenshot of a cell phone  Description automatically generated |

## Creating a Ticket (Logged in as Developer or Tester)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test ID | Description | Input | Expected Result | Screenshot |
| 1 | Date | N/A | Deny | A screenshot of a cell phone  Description automatically generated |
| 2 | Date | 06/11/2019 | Accept | A close up of a logo  Description automatically generated |
| 3 | Timestamp | N/A | Deny | A screenshot of a cell phone  Description automatically generated |
| 4 | Timestamp | 16:00:00 | Accept | A close up of a logo  Description automatically generated |
| 5 | Description of bug | N/A | Deny | A screenshot of a cell phone  Description automatically generated |
| 6 | Description of bug | “There is a logic error on line 16” | Accept | A screenshot of a cell phone  Description automatically generated |
| 7 | Name of founder | N/A | Deny | A screenshot of a cell phone  Description automatically generated |
| 8 | Name of founder | “Dave” | Accept |  |
| 9 | Assigned to | N/A | Deny | A close up of a logo  Description automatically generated |
| 10 | Assigned to | “Developer” | Accept | A screenshot of a cell phone  Description automatically generated |
| 11 | Priority Value | N/A | Deny | A close up of a logo  Description automatically generated |
| 12 | Priority Value | Any value from: low, medium or high | Accept |  |
| 13 | Status Value | N/A | Deny |  |
| 14 | Status Value | Any value from: open, resolved or closed | Accept | A close up of a logo  Description automatically generated |
| 15 | Type Value | N/A | Deny | A close up of a logo  Description automatically generated |
| 16 | Type Value | Any value from: Development, Production or Testing | Accept |  |

## Creating a Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test ID | Description | Input | Expected Result | Screenshot |
| 1 | Comment | N/A | Deny | Not Implemented |
| 2 | Comment | “This is a comment” | Accept | Not Implemented |
| 3 | Comment Timestamp | -06-11-2019 16:00:00 | Deny | Not Implemented |
| 4 | Comment Timestamp | 06/11/2019 16:00:00 | Accept | Not Implemented |
| 5 | Comment creator | N/A | Deny | Not Implemented |
| 6 | Comment creator | “User12” | Accept | Not Implemented |
| 7 | Ticket status | N/A | Deny | Not Implemented |
| 8 | Ticket Status | Any value from: open, resolved or closed | Accept | Not Implemented |
| 9 | Ticket Status: Open | “This is a comment” | Accept | Not Implemented |
| 10 | Ticket Status: Resolved | “This is a comment” | Accept | Not Implemented |
| 11 | Ticket Status: Closed | “This is a comment” | Deny | Not Implemented |

## Database Access

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test ID | Description | Input | Expected Result | Screenshot |
| 1 | Encrypted passwords | Viewing password fields | Qwe548495bbjd73lkshjgf | A screenshot of a cell phone  Description automatically generated |
| 2 | Logging into the application | Incorrect Username  Correct Password | Deny | A screenshot of a cell phone  Description automatically generated |
| 3 | Logging into the application | Correct Username  Incorrect Password | Deny | A screenshot of a cell phone  Description automatically generated |
| 4 | Logging into the application | Correct Username  Correct Password | Accept | A screenshot of a cell phone  Description automatically generated |
| 5 | Encryption of tickets | Viewing tickets | 43i5uhfniuf893r4f98nw | Not Implemented |
| 6 | Encryption of comments | Viewing comments | 8237tfb87c73y87fddew | Not Implemented |
| 7 | Account Lockout | Correct username  Incorrect password | Deny | A close up of a logo  Description automatically generated  A screenshot of a cell phone  Description automatically generated |