# Hajj Portal

This report gives an overview of the Hajj electronic portal for Al-Hajj applications. It includes data validation, security analysis, threat modelling, and protection tools to ensure application security. The report also evaluates the testing methods used for security.

**A Complete and Fully Functional Application**

The Hajj electronic portal allows pilgrims to securely apply for Al-Hajj and submit personal information. The submission form includes details such as Iqama number, name, contact, companions, package company, and comments etc. Pilgrims can modify or update their application, and package companies can approve or reject applications using a drop-down list.

**Security Requirement Analysis**

The security requirement analysis of the application identified the potential security risks and ensured that the application meets the security requirements. The application is designed to ensure the confidentiality, integrity, and availability of data. The application meets the authentication and authorization requirements, ensuring that only authorized users have access to the application.

**Threat Modelling:**

The threat modelling process identified the potential security threats and vulnerabilities of the application. The identified threats were mitigated by implementing the necessary security controls and measures, such as data encryption, secure data transmission, and user authentication.

**Data Validation:**

The application implements data validation to ensure that the data entered by the pilgrims is correct and meets the required format. The application uses regular expressions and other data validation techniques to validate the data entered by the pilgrims.

**Write Queries that Suffer from SQL Injection:**

To test the security of the application, queries were written that suffer from SQL injection. The results of the testing highlighted the potential security risks associated with SQL injection attacks.

**Use Prepared Statements (Parameterized Query):**

The application uses prepared statements (parameterized query) to prevent SQL injection attacks. Prepared statements ensure that the data entered by the users is treated as data and not as part of the SQL query.

**Use of Store Procedure:**

The application uses stored procedures to ensure the security of the data. Stored procedures allow the application to execute a series of SQL statements as a single transaction, ensuring that the data is consistent and secure.

**Use Views Instead of Tables:**

The application uses views instead of tables at the time of login to provide an additional layer of security. Views provide a logical representation of the data and limit the data that is available to the user, ensuring that the data is secure and confidential.

**Test Results:**

The application was tested using a range of tools and techniques to evaluate the security of the application. The testing included fuzzing, SQL injection testing, and other security testing methods. The results of the testing highlighted the strengths and weaknesses of the application and provided recommendations for improvement.

**Code Protection Tools/Techniques:**

The application uses a range of code protection tools and techniques to ensure the security of the application. Code obfuscation, anti-debugging techniques, anti-tamper techniques, memory scrambling, code encryption, and code virtualization were implemented to ensure that the application is secure and resistant to attacks.

**Conclusion:**

The Hajj electronic portal application is a fully functional and secure application designed for the pilgrims to apply for Al-Hajj. The application meets the security requirements and implements a range of security controls and measures to ensure the confidentiality, integrity, and availability of data. The application was tested using a range