Requirements table

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Rationale/Security Goals |
| 1 | Database interface | All interactions with the database need to call the database interface (DBI) function to access the database for data addition, deletion, modification, and check. | The goal is to establish secure database access, through the design of DBI, such as special character filtering for input parameters, or use of the prepare of SQL statements in the DBI library to avoid direct string connections, thereby eliminating the risk of SQL injection. |
| 2 | Restful interface based on HTTPS | All external requests uniformly adopt the restful interface to complete the interaction between the user and the server, and the server and the third-party server. For example, the interaction between the travel application and the server of the hotel, such as sending reservation user information to the hotel. | The goal is to safely complete the information transmission on the Internet and protect travel application services from XSS and CSRF attacks. For example, you can add input parameter filtering for restful requests and add CSRF token. |
| 3 | Order management | Manage user orders, support order payment, and support cancellation order refund function. Payments are made by third parties, such as online banking or PayPal. | The goal is to complete a secure payment and refund service. What needs to be considered is that due to the use of third-party payment functions, the transfer information received by the hotel is all from the user, not from this application. Therefore, when the cancellation service occurs, the user PII needs to be sent to the hotel to match the hotel's order information and the hotel will refund. As the user information is involved, the user information will be encrypted (not a one-way encryption method, it needs to be decryptable), for example, using an encryption algorithm such as RSA. After the hotel party decrypts the user information, the order information is matched. |
| 4 | COVID-19 vaccination status inquiry | Ask the user whether to accept the inquiry about the vaccination status. If the user chooses to accept, the user information entered through the order will be checked on the government's vaccine registration website for the vaccine registration status, and the user will be marked (such as a health icon) and preferential policies are provided. | The goal is to encourage users to vaccinate. And through the application to track the user's vaccine status. Consult the user's consent and confirm the consistency of the data by accessing the data set provided by the government. The security of user data also needs to be protected, and encryption is needed. |
| 5 | Navigation | The user checks how to arrive at the hotel reservation function. Route planning is done by calling third-party navigation, such as calling google map. | The goal is to provide users with a convenient way to find the booked hotel. This involves the collection of user latitude and longitude information, and a prompt will be given when installing the application whether to share. But the location information will not be saved in this APP, it will only be called as a parameter. If the user is unwilling to share location information, the APP can also call a third-party navigation application. At the same time, this application only obtains the location information of the current mobile phone, it does not need to be associated with user information and is not stored in the background database. |