SQL Injection

As the website communicates to the database through SQL, SQL injections need to be considered. These attacks could be used to commit fraud, steal private information or malicious alter a person’s stay at the hotel.

A firewall can detect many attacks by blocking queries that are invalid or contain too many blocks inside a request. The SQL commands used in the deployment and functionality of this website are largely paramatised which mitigates the possibility to a greater extent.

Cross Site Scripting

Malicious client-side code can be injected into the webpage, causing issues that vary from minor annoyances to wide-scale security issues. They can be mitigated by content control such as validating HTML, or by linking the session cookies to the user’s IP Address.

Hacking

At present the reception interface (checking in and out, payments etc.), and the housekeeping page are both only protected by not being navigable from the main website architecture, to prevent them being exploited they would need to be restricted to people with the correct credentials (username and password).

Denial of Service

All websites are at risk of malicious action from groups simulating heavy traffic. A firewall can go some way to prevent attacks, also statistical models can be implemented to review traffic, particularly and the application level.