|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Risk Statement | Response strategy | Objectives | Likelihood | Impact | Risk Level |
| Hacking/  Pentesting | There are malicious scripts the brute force log in credentials this could result in the loss of personal data or the use of database information as data ransom in exchange for bit coin. | Ensure username and password to a more secure option (for example, not using root or admin). Or using SSH key or similar instead of passwords | Extend the duration for which the database’s security credentials will not be able to be discovered through brute forced using malicious scripts. | Medium | High | Medium–high |
| Repetitive Strain Injury | Extended periods of time inputting data and usage of the keyboard could result in strain on the joints of the hand and wrist resulting in injury and potential impact all further computer usage. | Take regular breaks in order to rest the muscles and tendons in the hands and wrist, define a maximum length of time allowed to work in one sitting. Ensure that the seating position is correct for reduced injury. Include gel pads to reduce strain | To remove the potential of injury, which in turn allows for the uninhibited continuation of the project, data entry. Ensure that required work its achieved-on time. | Low | Low | Low |
| SQL injections | Malicious injections of SQL statements into the inputs of the IMS could result in information leaks or the potential deleting all data in a table’s resulting in the loss of data. | Limit the number of characters able to be added into the input prompts, filter all special characters before submitting the query. | Prevent inevitable use of SQL injections by using the IMS. Reducing the impact on the potential data leak/loss | High | High | High |
| Data Leaks | The use of incorrect data access modifiers for different variables and classes in the Java code can result in the access of private information to all. The data leaks could be used for ransom or blackmail depending on the value of the leaked data. | Ensure that each access modifier is set to the correct level, using private when appropriate to ensure that sensitive information is inaccessible to the user. | Limit the amount of information able to be accessed or discovered when using the IMS, keeping private details inaccessible. | Medium | Low | Medium-Low |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Risk Statement | Response strategy | Objectives | Likelihood | Impact | Risk Level |
| Jenkins | The use of weak passwords could allow a malicious user to run bash commands directly on the computer hosting Jenkins. | Ensure that all passwords are strong and changed every 3 months. | Prevent the threat that could result the computer being used for malicious uses. | Low | High | Med |
| GitHub | Source code published on to GitHub could provide hackers with insight into how to attack software running in production. Code and supporting files pushed onto GitHub could mistakenly contain login credentials for other services allowing access to other services and leaking data from those services. | Make the github repository private so that non of the code is visible to the public and protecting IP. | Reduce the likelihood of being prevent leaking of data and personal information from other sites when login credentials are hard coded into the pushed files to GitHub. | Medium | High | Medium-High |