Description	Evaluation	Likelihood	Impact	Responsibility	Response	Control Measures
Database could be accessed by an outsider	All tables could be deleted and the data permanently lost	Medium	Medium	Database Administrator	Recover from backup if possible. Identify weakness exploited to gain entry and add extra security.	Create regular backups (daily) of the database. Preform regular security reviews to assess the eases of outside accessibility. Change password at regular intervals to prevent a brute force attack.
GitHub repository could become compromised	Secret information such as API keys could become exposed	Medium	Medium	Repository Owner	Assess repository accessibility and who is enables as a contributor. Check what information is being stored on the repository.	Move all secrete information out of the repository and into the deployment tools (Jenkins) so that if the repository is compromised secret information is not exposed.
A developper could introduce a bug to the master branch and deploy to production	The live production environment could contain a bug that causes failure at runtime	Medium	Medium	DevOps Engineers	Redeploy a previous version of the master branch and create a new patch branch to solve the issue	Use test validation during deployment to catch any code behaving unexpectedly. Setup jira to support high priority bug fixes so developers can prioritise major issues.
Hand and eye strain	Prolonged use of a keyboard/mouse and a monitor can result in discomfort and pain for developers	High	Low	Individual Developers	When a developer begins to feel discomfort they should immediately take a break and rest before they continue to work	Allow staff to take regular hourly breaks away from the computer to let developers bodies rest from continued use of I/O devices