|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Description | Assessment | Risk | Impact | Responsibility | Current Mitigation | Proposed Mitigation | Response | Tolerance |
| DDOS (Distributed Denial Of Service) attack | A DDOS, being a cyber-attack will disrupt the services of a host connected to the internet. Giving an error of service being unavailable this will cease access and functionality of the application. | Low | High | Kholeo Taylor |  | Constant monitoring of the application can prevent significant damage, seeing if spikes occur that can identify a start of a potential DDoS attack.  Over providing bandwidth can give some scope to address a DDoS before it gets high risk giving enough time to react in the event it may occur.  Limiting Requests through a filter to drop half open connections, identifying the threat and ignoring potential damaging packets of data. | Keep backups of the application and database and choose a host which is reliable and responsive in that situation.  Another domain can be booked in an event that the uptime is critical for the application allowing for backups to be uploaded to the other domain while the primary is down doing a forward/redirecting from the primary domain, still allowing visitors and negating from negative brand reputation. |  |
| SQL Injection | Malicious SQL code can be used for backend database manipulation to access information that was no intended to be displayed. A successful attack will result in the unauthorised viewing of user lists, deletion of entire tables and gaining administrative rights to the database | Low | Medium | Kholeo Taylor |  | The application can be regularly updated to avoid security flaws from being found in the software. The implementation of validation techniques can be applied, avoid building databases commands as strings that are joined from user input but instead using prepared statements. | Immediately shut down the server if a breach was to happen and notify all the users that it has happened, this will be in a form of the contact details they have left (email) instructing them on the stages of staying protected by changing their passwords in a more secured way |  |
| Social Engineering | Users on the application may use social engineering as a way of gaining information in a manipulative way | Medium | Medium |  |  | Set a terms and agreement in which the users will have to abide by in any even its broken their access to the application will be revoked as stated in the guidelines | Investigate and remove users who abuse the application for ulterior motives, to administrate and monitor the community of the application to make sure it is used properly and keep the sense of security for the users that want to use the website. |  |
| Cross Site Scripting (XSS) | An application-layer web attack that targets scripts executed on the client side rather than the server side. It manipulates client-side scripts of a web application to execute in a manner desired by the malicious user, it can be executed any time the page is loaded or when an associated even is performed. | Medium | High |  |  | To escape text and to validate user input, can be done using flask to use an extension  Web server can be set to redirect invalid requests, detect simultaneous login and invalidate sessions.  Enact various aspects of the Content Security Policy |  |  |