Edition 3:

STRIDE is technically a taxonomy and mnemonic for threats. It stands for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Below is how we apply STRIDE to our project.

1) Spoof. Some users may enter the system without authorization. They may do this by stealing login credentials or exploiting weak authentication. To mitigate this, we can enable two-factor authentication and design a rule to ensure users keep their credentials safe.

2) Tampering. Someone may change or delete the course rules, user-defined rules, or database entries incorrectly, which will affect the data integrity of the system. To mitigate this, we can set some restrictions on the modification of some rules or database entries, in case the user compromises data integrity.

3) Repudiation. Some users may deny some actions they have ever taken. It may be because they forget it or because they want to avoid taking responsibility for the wrong actions. To mitigate this, we can record the history of each modification and, if an issue arises, enable the system to roll back to the previous version.

4) Information disclosure. Some sensitive information may be leaked, for example, undisclosed unit and course information and private information from employees and students. To mitigate this, we can encrypt sensitive data at storage and in transit. Make sure the users can only have access to the data they need.

5) Denial of service. The application and database may be attacked by a DoS attack, which will lead to a failure in the system or some vital functionality. To mitigate this, we can deploy protection for the attack from the network, such as a firewall. Setting the caching as a buffer for the large number of requests in a short period of time, which will enable the system to adapt to the dynamic load.

6) Elevation of privilege. A user with limited privileges may have access to some high-level content by exploiting the vulnerability of the system. To mitigate this, we can review and update privilege settings regularly. Make sure the users only have access to the content they absolutely need.