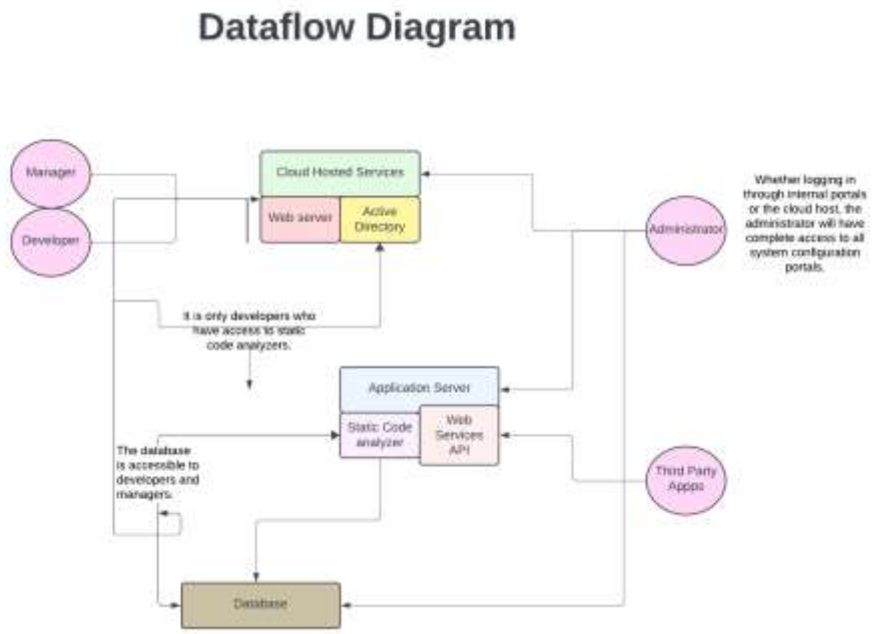
Credit task 1.3C: STRIDE Threat modelling



Whether logging in through internal portals or the cloud host, the administrator will have complete access to all system configuration portals.

It is only developers who have access to static code analyzers.

The database is accessible to developers and managers.

Submit one PDF file including the STRIDE threat modelling table.

Threats	**List of threats and their impacts**	**Mitigation**
Spoofing	* Attackers may impersonate developers, managers, or administrators in an attempt to undermine the web application's security measures.	* Strong password policies should be implemented for all apps, and multi-factor authentication should be used when appropriate. As effective keys for access control, OAuth and secure session tokens can be employed.
Tampering	* This implied that techniques like altering the supplied code or analysis results could jeopardize the integrity of the vulnerability scan data.	* Encryption (TLS/SSL) or hashing/signature methods on the data can both adequately serve data integrity. Access controls, audit logging, and other methods should be chosen in order to gather evidence of tampering.
Repudiation	* Accountability concerns might arise, for example, if a particular network user worked on altering the vulnerability status or uploading code, and upon being questioned, that person denied doing so.	* Forbid time-stamped user activity tracking and audit all user interactions. To make sure that logs cannot be edited, it is essential to make sure that append only systems are used.
Information disclosure	* Vulnerabilities or private information may be made public by users or/and third parties who have access to scan results or other sensitive user data (stored in the database or obtained using an API).	* Use encryption to improve security for both data at rest and data in transit. Use the idea of role-based access control, or RBAC, to manage the problem of access to knowledge that needs to remain restricted within an organization. Make sure that granting access credentials is done on a regular basis.

Denial service	* An attack could attempt to overwhelm web servers or application servers, preventing authorized users from performing static code analysis.	* Insist on using traffic filtering, rate limiting, and web application firewalls on the Internet. The cloud service provider may additionally offer this solution by utilizing DDoS protection services.
Elevation of Privileges	* A user with restricted access (like a developer) might take advantage of this vulnerability to elevate their privileges to administrator level, which could have a detrimental impact on the entire application.	* Code reviews and penetration testing are examples of implemented consistent security testing. Make sure you are committed to honing your sandboxing skills and that you strictly enforce access control policies. In all actions, the least privilege concept should be adhered to for proper access to jobs.