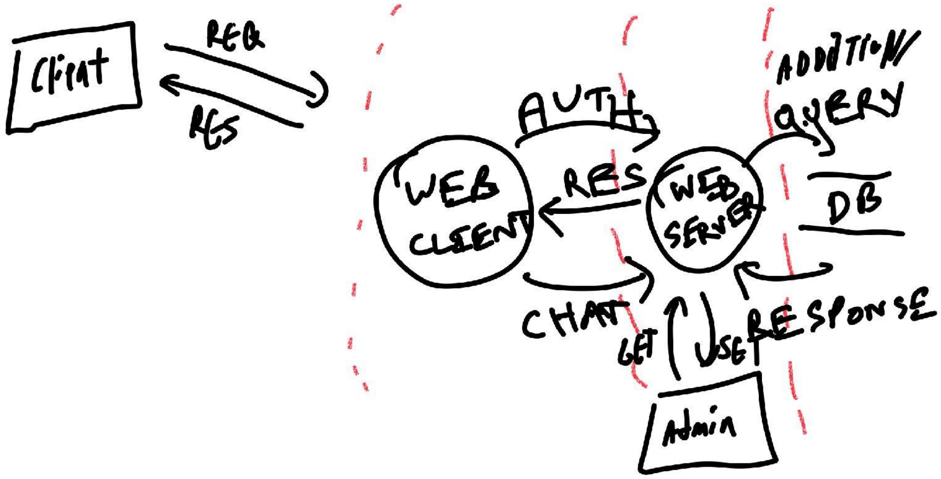
STRIDE Analysis of DLN

Eric Neidhart, Ankit Sanghi, Ginnie White

Data flow diagram for DLN:



1. Spoofing:
    - An attacker could impersonate a user to gain access to their profile information such as credit card information, etc: To prevent this, we make the user use a secure password (long alphanumeric) as well as two-factor authentication (Duo Mobile or similar).

2. Tampering
    - A Malicious admin could tamper with the database to modify lemur information: We can mitigate this by having all changes (and records of people who made those changes) be logged to a read only database, and/or have all changes be approved by multiple admins.
    - An attacker may use input text boxes (such as the chat function or search functions) to attempt code injection attacks against the system: this can be mitigated by ensuring that all user input is sanitized/not read as code.

3. Repudiation
    - An attacker performs a malicious action on the system: Any and all actions made by any user are recorded in a read-only database so that if any malicious acts are performed, the user who performed the action is recorded and the admins are notified.

4. Information disclosure
    - An attacker may attempt to intercept authentication details and other information: All communications should be done using a secure system such as TLS and HTTPS.
    - A hack on the database containing authentication details may allow attackers to gain access to confidential information. All passwords should only be stored in cryptographic hash form along with the method of hashing.

5. Denial of Service
    - An attacker may perform a DDOS attack to prolong the lemur menace: The web service should have some form of DDOS protection such as Cloudflare Inc.

6. Elevation of Privilege
    - Malicious attacker is elevated to admin status: Being elevated to admin comes with a probationary period where other admins of higher status are notified and may terminate that elevation if it is invalid.