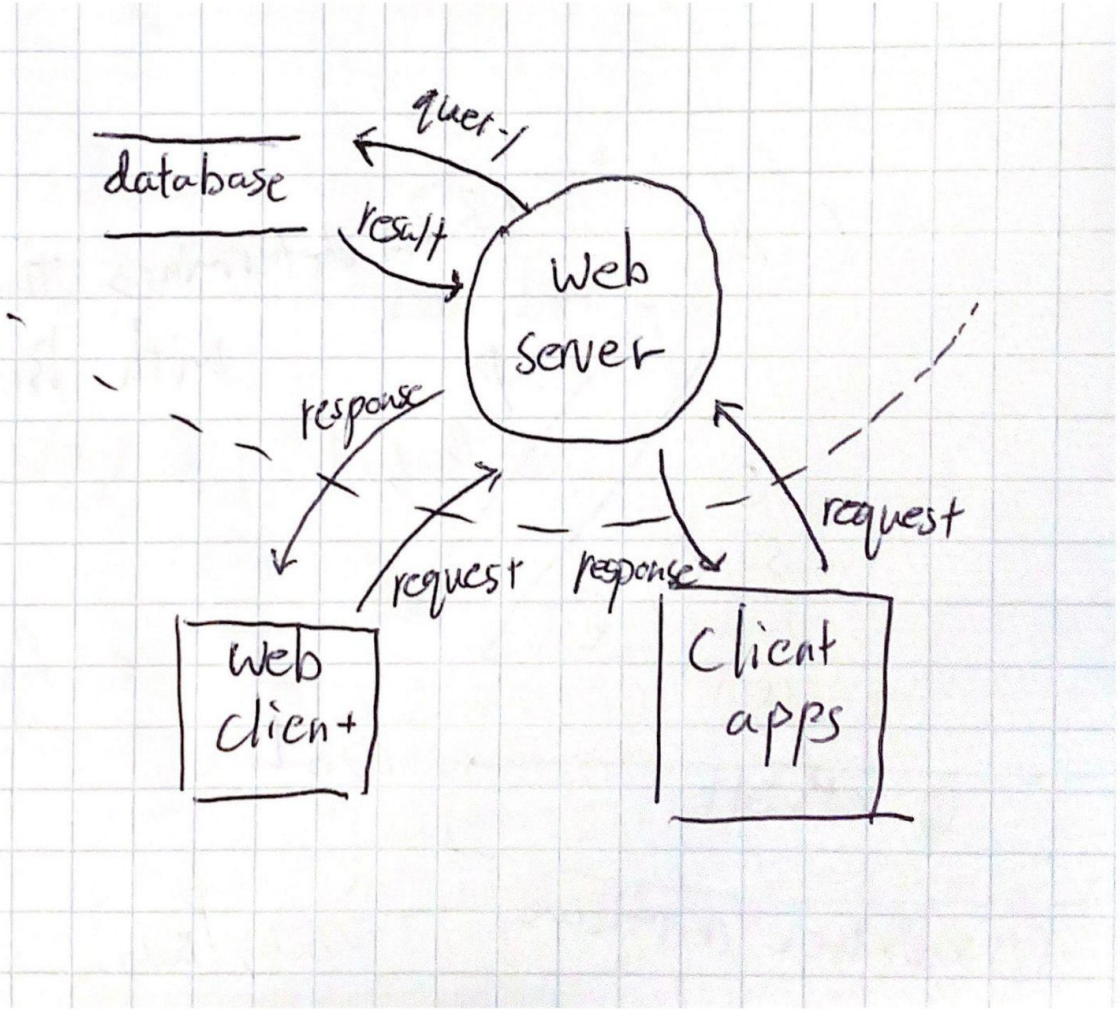
Aiden Chang, Sean Lee

- Spoofing
    - Users can use spoofing software like Ettercap to bind the attacker's MAC address to the IP address of the victim's gateway so that the traffic is then redirected to the attacker. One simple corresponding mitigation could be the required use of VPNs.
- Tampering
    - Malicious viewer views or tampers with personal data en route from the Web server to the client or to the client from the web server. Corresponding mitigation could be having all interactions occur over HTTPS
- Repudiation
    - A user can log in to another user and tamper with their posts and chats. Corresponding mitigation could be having a 2 step verification log in.
- Information disclosure (privacy breach or data leak)
    - Can use SQL injection to retrieve data that should not be available to the user. Corresponding mitigation is to use correct input string formatting when sending the query to the database.
    - A database breach will expose all the information of an account. Corresponding mitigation is to encrypt the password and store the encrypted version.
- Denial of service
    - Denies access to the database server by flooding it with TCP packets. Corresponding mitigation is to limit the number of TCP packets sent per minute.
- Elevation of privilege
    - A user can upload a file that contains a trojan program that gives them admin privileges allowing them to retrieve private information for the members. Corresponding mitigation is


database
query
result
Web server
response
request
request
response
Web client
Client apps