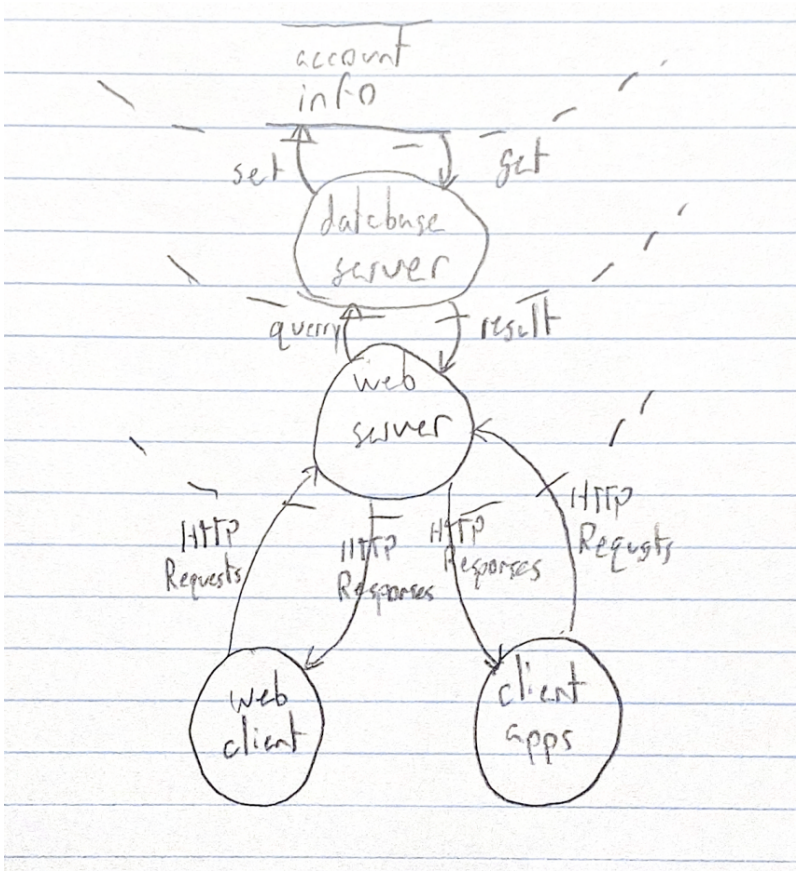
Miles Hoene-Langdon

Data Flow Diagram:



Threats and Mitigations:

- (Spoofing) A phishing attack where the attacker pretends to be the webserver in order to trick users into giving the attacker their login credentials. One possible mitigation is requiring two-factor authentication, so even if login credentials are obtained, they cannot be used to access the user's account.
- (Spoofing) An adversary in the middle attack where the attacker tricks the client and server into thinking they are talking directly to one another, when in actuality the attacker intercepts all the information in between. A mitigation for this attack is using proper encryption techniques like Diffie-Hellman along with public/private keys of the server to verify that the keys match and that there is no adversary in the middle reading and potentially altering the information.
- (Tampering) An attacker modifies HTTP requests by the client for changing a user's password and associated email address. This tampering then locks the user out of their account as the address that reaches the database server and the password are not what the user knows. A mitigation for this is using secure encryption like HTTPS to make

successful tampering difficult. If the attacker doesn't know what the contents of packets are, they cannot tamper with them in a meaningful way like in this scenario.

- (Repudiation) An attacker impersonates a user that is not themself to try and coerce someone into giving them their login credentials. This impersonation tricks the server, so they don't know that these actions came from the attacker. A mitigation of this attack is creating specific user IDs and keeping track of more specific information, so that impersonating another user is extremely difficult to pull off.
- (Information Disclosure) An eavesdropper intercepts queries and results sent between the database server and the web server gaining information about users requests and results from the server. A mitigation of this attack is using HTTPS for communication between the webserver and database server. This encrypts the requests and results, keeping users' information confidential.
- (Denial of Service) An attacker sends a ton of packets to the web server for their computer, which overload it and prevent other users from accessing the service of the website. A mitigation of this attack would be having a protocol in place that prevents users from sending any amount of packets that exceeds a fixed limit. This would limit the user overloading the server, by ignoring all packets sent after the fixed limit. This would then allow others to successfully use the service as the server is no longer overloaded.
- (Denial of Service) An attacker sends a bunch of packets to the web server from various different spoofed IP addresses. This overloads the web server and denies service to other users while keeping the attacker hidden. A mitigation for this attack is creating a system of filtering packets based on a set of rules used to identify DDoS tools, in order to block packets that resonate with these rules.
- (Elevation of Privilege) An attacker sends an email to the computer with the database server that contains malware. This malware gives the attacker privileged unauthorized access to account information. A mitigation for this attack is having good antivirus software on the database server computer and making sure to only open emails from known sources.