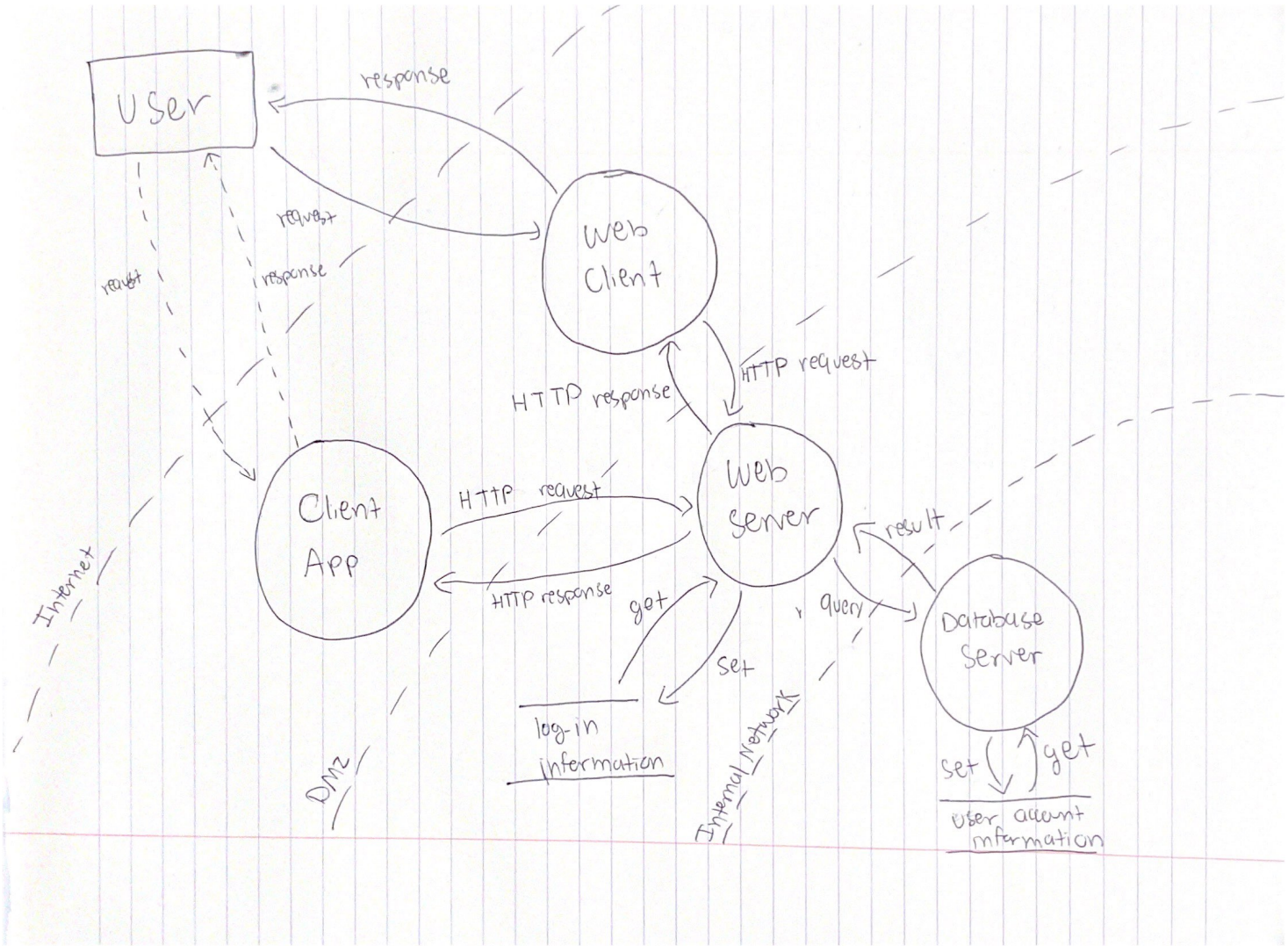
User
response
request
request
response
Web Client
HTTP request
HTTP response
Client App
HTTP request
HTTP response
Web server
result
query
Database Server
get
set
log-in information
set
get
User account information
Internet
DMZ
Internal Network

Miguel Alvarez, Fabricio Rua-Sanchez

Threats and Mitigations:

- It was not specified that the web server had a certificate from a CA, so anybody could use ARP poisoning to act as a PITM. (Spoofing)
    - Mitigation: get a certificate from a CA in order to ensure that the user can confirm the identity of the web server.
- Phishing is dangerous because if an admin were to click on a malicious email, this could give the malicious actor higher access to restricted parts of the service. (Spoofing)
    - Mitigation: Requiring two-factor authentication in order to mitigate the damage of a successful phish. This ensures the identity of the person attempting to login.
- Assuming that the login information is stored within the web server, if this were to be hacked the login credentials of users would be easily able to be tampered with. (Tampering)
    - Mitigation: By using a hash function for the login credentials (something such as SHA-256 which is a one-way function) this could prevent any malicious actor from ‘reversing’ the data stored(i.e. login credentials).
- If the attacker uses SQL injection attacks to do invalid requests this tampers data. (Tampering)
    - Mitigation: Use stored SQL procedures
- If a malicious actor has unlimited login attempts, then they could use brute force to guess login credentials. This would allow them access to private information. (Repudiation)
    - Mitigation: The user should be locked out of their account after x amount of attempts where they are sent an email to reset their password.
- If we assume that the password is not encrypted (for example using Basic Authentication) then if there is a data breach, the leaked information would violate user confidentiality. (Information Disclosure)
    - Mitigation: The data stored should be encrypted (using any asymmetric or symmetric encryption method).
- If a malicious actor sent way too many requests to the server to the point where the server couldn’t keep up with the incoming requests, then this makes the system vulnerable to other attacks. (Denial of Service)
    - Mitigation: We can use blackholing to route the incoming traffic to a null server which doesn't negatively affect the main server.
- If an attacker changes their membership to a higher role then this poses problems since they would have access to restricted information/data. (Elevation of Privilege)
    - Mitigation: Expiring passwords for administrators/accounts with administrative privileges.