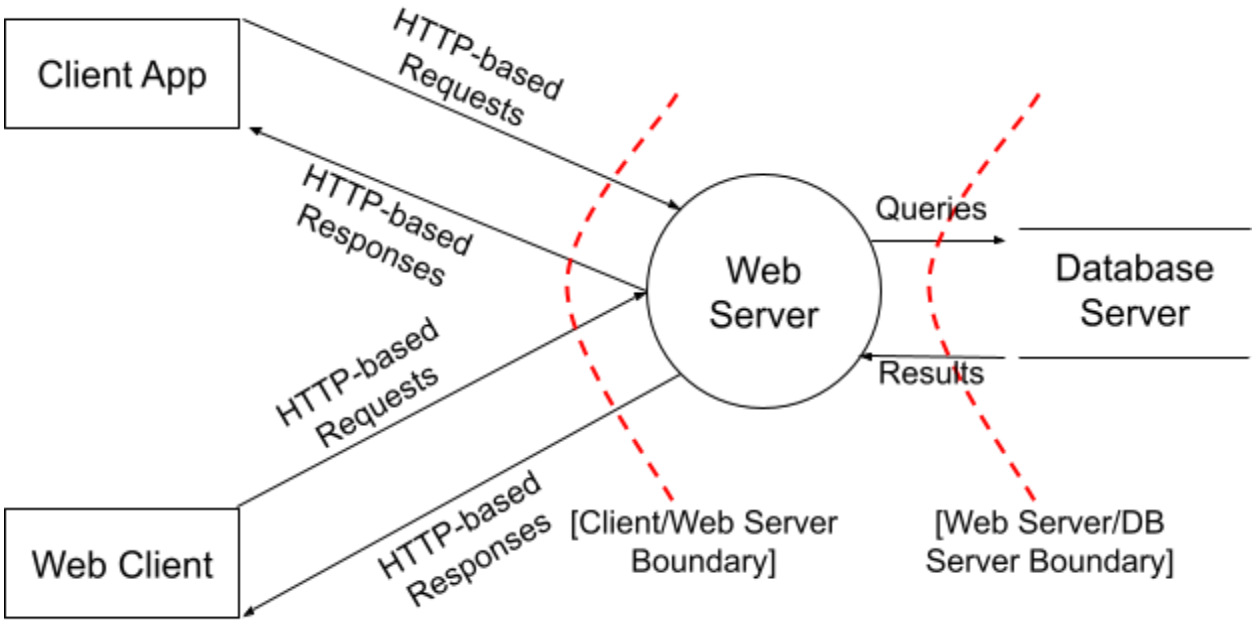
Author: Kyle Machalec

Data Flow Diagram



STRIDE analysis

- Spoofing
    - A user impersonates another user by creating an account that goes by the same name, spreading tapir hate messages under the impersonated individual's name.
        - Mitigation: Require that users choose a unique username at account creation
    - A hacker steals the username and password of a Tapirs Unlimited user, logs into their account, and changes the password. Now the hacker can impersonate the original user while the original user is no longer able to access their account.
        - Mitigation: Require that users link their Tapirs Unlimited account to their email. Any password change request must first be verified through the email associated with the account.
- Tampering
    - A malicious entity could intercept and change data as it flows between the user's network and the web server. As a result, the malicious entity could display false information about tapirs on the user's device.
        - Mitigation: Ensure that all communication between the user and web server is done using HTTPS
- Repudiation
    - A user denies that they spread hateful speech in a forum
        - Mitigation: Require digital signatures for any client-server communication and record relevant information about any user's forum posts such as timestamp and user IP address. Timestamps can be compared to the

records of outgoing packets on the user's machine. If approved by a court, the user's ISP can be asked to reveal the identity of the person associated with the given IP address.
    - A user denies that they made a large purchase of tapir merch
        - Mitigation: Same as previous scenario (digital signature, timestamp, and IP address are all useful for finding the identity of the buyer)
- Information disclosure
    - An attacker uses a SQL injection to send malicious code through user input that tricks the database into returning potentially sensitive information outside of the search function's scope.
        - Mitigation: Use parameterized queries including prepared statements and input validation
    - An eavesdropper on the user's network reads the password sent from the client to the server.
        - Mitigation: A hashed version of the password is stored in the database and compared to the hashed version of the password sent by the user.
    - An eavesdropper listens in on direct messages sent between two tapir enthusiasts.
        - Mitigation: End-to-end encryption using RSA and AES with messages sent between two users
- Denial of service
    - Hackers use a DDoS attack on the Tapirs Unlimited server.
        - Mitigation: Use rate-limiting to accept as much traffic as the web server can handle without affecting availability and only accept traffic that is legitimate by analyzing the individual packets sent by the client. It could also be helpful to increase server capacity.
    - A malicious individual creates a program that generates thousands of fake accounts to overload Tapirs Unlimited's server.
        - Mitigation: Use CAPTCHA at account creation
- Elevation of privilege
    - An admin, either with Linode or Tapirs Unlimited, could have their password stolen (i.e. they use the same password on many sites and one site has a data leak). As a result, an unauthorized individual finds themselves with the credentials to gain admin access.
        - Mitigation: Require admins to change their password frequently and use two-factor authentication
    - A hacker guesses the session ID of an admin, allowing them to enact changes to the website.
        - Mitigation: Ensure session IDs are long and are created by a cryptographically secure pseudorandom number generator