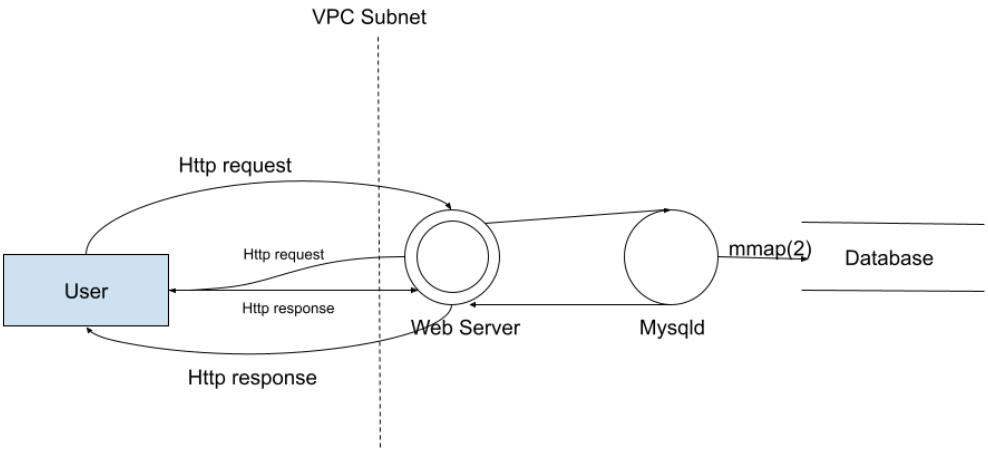
Security Design Review
Authors: Garrett Phillips, Benjamin Boardley, Jack Gardner
Course: ECE49595O - Spring 2024
Date: 04/05/2024



1.
2. Below are listed 2 threats to us and our users that are present within our project.
    a. The JWT tokens used for our authentication system. JWT are notoriously insecure and can allow attackers to bypass controls, and impersonate users. This can also allow attackers to send modified JWTS to the server with malicious intent.
    b. During deployment through the use of an AWS EC2 instance, there are security risks associated with attackers gaining access to our backend servers through ssh. This would expose sensitive client information that would be harmful to our users.
3. Below are detailed descriptions of mitigations for the threats listed above.
    a. A mitigation to this threat is to sign or encrypt the token, with a decided upon algorithm. This algorithm will be located in the claims header. If the algorithm is listed as none that means that it is not signed at all and should not be accepted. Elliptic curve-based algorithms are typically considered more secure.
    b. This security risk is most mitigated through AWS' built-in cloud security for its' EC2 instances but is still vulnerable if not handled correctly by the admin (us). We can mitigate this risk by controlling and giving specialized network access to our EC2 instances through the configuration of our VPC and its respective subnets. These VCP subnets allow for a range of IP addresses that have access to the instances. The VCP also comes with default security groups, which further enhance the security. This risk can also

be mitigated through the use of IAM rules, which manages AWS credentials to the instances. Although, these credentials need to be updated on each instance, which for early development may be a tedious and unneeded process.